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

Adriana Elissa Notoy

IARSDE - Infra Estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos: Validade do documento eletrônico por tempo indeterminado

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
custodio@inf.ufsc.br

Florianópolis, Março de 2002

IARSDE - Infra Estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos

Adriana Elissa Notoya

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

Prof. Fernando Ostuni Gauthier, Dr.
Coordenador do Curso
gauthier@inf.ufsc.br

Banca Examinadora

Prof. Ricardo Felipe Custódio, Dr.
Orientador
custodio@inf.ufsc.br

Prof. Aires José Rover, Dr.
airesjr@dcj.ufsc.br

Prof. Luiz Carlos Zancanella, Dr.
zancanel@inf.ufsc.br

Prof. Ricardo Dahab
rdahab@ic.unicamp.br

Um homem precisa viajar, por sua conta, não por meio de histórias, imagens, livros ou TV. Precisa viajar por si, com seus olhos e pés, para entender o que é seu, para um dia plantar as suas próprias árvores e dar-lhes valor. Conhecer o frio para desfrutar o calor, e o oposto, sentir a distância e o desabrigo para estar bem sobre o próprio teto. O Homem precisa viajar para lugares que não conhece, para quebrar essa arrogância que os faz ver o mundo como imaginamos e não simplesmente como é. Que nos faz professores e doutores do que não vimos, quando deveríamos ser alunos e simplesmente ir ver. (Amyr Klink)

Aos meus pais.

Agradecimentos

Aos meus pais, pelo estímulo e apoio incondicional desde a primeira hora; pela paciência e grande amizade com que sempre me ouviram, e sensatez com que sempre me ajudaram.

Ao professor Ricardo Felipe Custódio, o meu mais sincero agradecimento, a minha estima e consideração por seu valoroso trabalho junto ao LabSec e pela oportunidade dada de desenvolver este trabalho sob a sua orientação.

A minha irmã Luciana, que sempre esteve presente, demonstrando muito carinho e atenção, e me dando forças para superar cada novo obstáculo. Ao meu irmão Elthon, um amigo que meu deu um grande presente: minha sobrinha Emilly. A minha prima Cris pelo companherismo, amizade e presença afetiva com que me recepcionou em sua casa.

Ao constante apoio recebido de uma pessoa admirável, Sirlei, que acreditou e investiu em meu potencial e acima de tudo pelo grande valor da sua amizade.

Aos amigos Anderson, Everton, Genilda, Gláucio, Maria, Roberto e Sônia que estiveram presente durante o mestrado, ajudando-me e incentivando-me em diversos momentos. E a um amigo especial, Marcos Padilha, o qual sempre prestou um grande incentivo nas minhas buscas por crescimento tanto pessoal quanto profissional.

Ao meu namorado Fernando, pela compreensão e atenção dada nas longas horas que este trabalho exigiu, e principalmente pelos grandes momentos proporcionado por sua companhia.

E acima de tudo a Deus, responsável por todos acontecimentos e pelo encontro com todas essas pessoas especiais na minha vida.

Sumário

Lista de Figuras

Lista de Siglas

AC	Autoridade Certificadora
AD	Autoridade de Datação
AGT	Autoridade de Garantia de Tecnologia
ASN.1	Abstract Sintax Notation One
DSS	Digital Signature Standard
DT	Data Type Document
ETSI	European Telecommunications Standards Institute
GPEA	Government Paperwork Elimination Act
IARSDE	Infra Estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos
HTML	HyperText Markup Language
K	Chave simétrica
KR	Chave privada
KU	Chave pública
PDDE	Protocoladora de Datação Documento Eletrônicos
SGML	Standard Generalized Markup Language
TTS	Trusted Third Party
XAdES	XML Advanced Electronic Signatures
XAdES-T	XAdES com Time-Stamp
XAdES-C	XAdES com Dados de validação completos

XAdES-X	XAdES com Dados de validação eXtendidos
XAdES-X-L	XAdES-X com Assinatura
XAdES-A	XAdES-X-L com dados de validação para arquivo
XML	Extensible Markup Language

Resumo

Este trabalho apresenta uma dissertação de mestrado em Ciência da Computação da Universidade Federal de Santa Catarina, na linha de pesquisa de Segurança e Comércio Eletrônico, vinculado ao **LabSEC** - Laboratório de Segurança em Computação.

A proposta apresentada neste trabalho constitui-se de uma infra-estrutura de armazenamento e recuperação de documento eletrônicos, que garante a estes a retenção de seus atributos por tempo indeterminado.

A infra-estrutura atualiza dinamicamente a tecnologia utilizada para conferir a assinatura digital e o selo de tempo. Para que isto seja possível, neste trabalho consta também uma proposta de software padrão de assinatura digital, o qual organiza o documento e suas informações de modo a garantir a Infra Estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos - IARSDE os atributos necessários para o controle da renovação da tecnologia do documento.

Palavras-chave: criptografia, assinatura digital, documento eletrônico, validade jurídica.

Abstract

This work presents a Computer Science Master's Degree Dissertation of Universidade Federal De Santa Catarina, in the research line of Electronic Commerce and Security, linked to LabSEC - Laboratório de Segurança em Computação (Computer Science Security Lab).

The proposal presented in this work consists of an electronic document storage and recovery infrastructure, which guarantees, thanks to these items, the retention of its attributes during an arbitrary period of time.

The infrastructure updates dynamically the technology used to confer the digital signature and timestamp. In order for this to be possible, within this paper there is also a proposal for standard software of digital signature, which organizes the document and its information in such a manner that it guarantees the IARSDE - the necessary attributes for the renewal control of the technology of the document.

Keywords: cryptography; digital signature; electronic document; juridical validity.

Capítulo 1

Introdução

O crescimento dos serviços oferecidos pela Internet e o número de pessoas que a utilizam, resultou em um aumento no uso de documentos na forma eletrônica.

As informações constantes nesta forma de documento vão da simples trocas de mensagens a dados sensíveis, como números de cartões de crédito, dados bancários e acordos comerciais. Estes, por sua vez, necessitam de sistemas de segurança para garantir não somente que a visualização ocorra apenas entre as partes comunicantes, mas também que assegurem os atributos necessários de cada tipo de transação.

Nas transações comerciais realizadas através de documentos eletrônicos, a partir do momento que um cliente e o comerciante firmam um acordo, qualquer um que necessite da comprovação da ocorrência deste fato deve ser assegurado de evidências de prova.

Com a tendência da popularização do documento eletrônico, aliada à aprovação da medida provisória 2.200-2 em 2001, a qual regulamenta a assinatura digital no Brasil, o estudo dessa nova forma de representação torna-se de grande valor.

Assim, o conteúdo desta dissertação consiste em uma pesquisa visando a identificação dos elementos mínimos e indispensáveis aos documentos, de forma a estudar e propor mecanismos e ferramentas para que estes sejam proporcionados aos documentos eletrônicos e possam ser acolhidos juridicamente. Essa pesquisa não se atém a peculiaridades ou requisitos específicos dos tipos de documentos juridicamente exis-

tentes, tratando as características comuns e aplicáveis a todas as espécies.

1.1 Objetivos

1.1.1 Objetivo Geral

Propor uma infra-estrutura para garantir autenticidade e integridade de longo prazo de documentos eletronicamente assinados.

Uma primeira forma de resolver o problema do objetivo geral deste trabalho é criar-se novos métodos de assinatura digital, que tenham um maior tempo de durabilidade tecnológica.

Porém, a realização destes métodos propostos na literatura continuam a definir um tempo limitado para a tecnologia.

Este trabalho utiliza uma abordagem diferente para resolver o problema. A idéia básica é controlar o tipo de validade da tecnologia utilizada para assinar o documento e substituir dinamicamente esta tecnologia e autenticidade, por uma outra tecnologia mais moderna quando necessário.

1.1.2 Objetivos Específicos

- Definir o que é um documento eletrônico;
- Levantar a legislação sobre a validade jurídica do documento eletrônico;
- Fazer uma revisão bibliográfica sobre assinatura digital;
- Levantar as propriedades tecnológicas de um documento papel que permitem estabelecer sua validade jurídica;
- Verificar o aspecto temporal do documento eletrônico em relação à data de criação e tempo de validade;
- Realizar uma análise comparativa dos documentos nas formas papel e eletrônica e levantar os requisitos necessários para conversão entre ambas;

- Estabelecer os critérios necessários para a validade jurídica da cópia impressa de um documento eletrônico;
- Estabelecer os critérios para que documentos na forma papel mantenham suas propriedades na migração para forma eletrônica;
- Fazer uma revisão bibliográfica sobre os principais métodos de codificação de documentos eletrônicos;
- Analisar os atributos legais do documento papel e identificar e/ou propor métodos que proporcionem esses atributos aos documentos na forma eletrônica;
- Pesquisar leis no âmbito mundial sobre a adoção e incentivo do uso do documento eletrônico;
- Levantar a existência de padrões e normas de codificação e/ou especificação de documentos eletrônicos;
- Estudar os métodos existentes para conversão entre formatos de codificação de documentos eletrônicos;
- Estudar o processo de verificação da validade de um documento eletrônico;
- Propor uma infra-estrutura de armazenamento e recuperação de documentos eletrônicos que mantenha os requisitos do documento;
- Propor o desenvolvimento de ferramentas oficiais para auxiliar na validade jurídica de um documento eletrônico;

1.2 Materiais e Métodos

Este trabalho é uma pesquisa teórica para a qual foram utilizados os recursos bibliográficos e computacionais do Laboratório de Segurança em Computação -

LABSEC, da Universidade Federal de Santa Catarina - **UFSC**. Também encontra-se fundamentado em artigos científicos, dissertações de mestrados e livros na área de técnicas criptográficas.

Projetos e leis relacionadas ao documento, documento eletrônico e Infra-estrutura de Chave Pública, foram utilizados para dar embasamento a diversas definições relacionadas à área jurídica no desenvolvimento deste trabalho.

1.3 Trabalhos Correlacionados

Existem diferentes propostas que visam atender os requisitos de segurança de um documento eletrônico, tais como o uso de assinatura digital e o acréscimo de selo de tempo.

Relacionado ao problema de padronização dos documentos assinados digitalmente, o **ETSI**[1] apresenta propostas que incluem atributos que visam a garantia de integridade do documento por longo período de tempo.

Porém, dentre os materiais pesquisados, não foram encontradas propostas abrangentes, que garantissem todos requisitos tecnológicos mínimos necessários aos documentos eletrônicos e a forma como estes devem ser geridos.

1.4 Justificativa

Com o surgimento dos algoritmos de criptografia assimétrica, dois dos atributos fundamentais ao documento, sob o prisma jurídico, puderam num primeiro momento ser garantidos aos documentos eletrônicos: a autoria e a integridade.

A partir deste fato muitas pesquisas, tanto da área jurídica como da área computacional, têm sido voltadas no sentido da completa equiparação legal do documento eletrônico ao documento papel.

Os cientistas da computação tem como função prover mecanismos tecnológicos para suprir os requisitos inerentes ao documentos papel, os quais já possuem

[1] European Telecommunications Standards Institute - www.etsi.org

um embasamento jurídico elaborado, também para a forma eletrônica.

Um levantamento minucioso dos requisitos dos documentos papel, revela que ainda existem alguns requisitos no documento eletrônico que não possuem propostas efetivas. Um dos principais é o problema do tempo de validade da autoria garantida aos documentos eletrônicos ser dependente do não comprometimento da tecnologia utilizada, enquanto no papel esta é válida durante toda sua existência.

Uma das formas propostas para resolver o problema da limitação do tempo de validade é através de propostas de novos métodos de assinatura digital, que tenham um maior tempo de durabilidade tecnológica. Isso pode ser alcançado através do aumento do tamanho das chaves (pública/privada), da utilização de um algoritmo mais seguro, ou seja, que não exista criptoanálise eficiente e/ou que a dificuldade de quebra por força bruta seja maior.

Assim as propostas encontradas na literatura não apresentam uma forma efetiva para garantir a permanência do atributo de validade duradoura aos requisitos atribuídos pela assinatura digital, pois este atributo continua estando limitado a um intervalo de tempo, ou não apresenta uma forma de gestão eficiente.

Este trabalho utiliza uma abordagem diferente para resolver o problema. A idéia básica é controlar o tipo de validade da tecnologia utilizada para assinar o documento e substituir dinamicamente esta tecnologia e autenticidade, para uma outra tecnologia mais moderna quando necessário.

A proposta da IARSDE vem a contribuir no sentido de analisar e reunir as melhores propostas, com suas devidas adaptações, e ainda propor mecanismos para os requisitos que ainda não possuem soluções. Dessa forma, visa compor um ambiente que ofereça os requisitos mínimos necessários do documento papel ao documento eletrônico por longo período de tempo, apresentando soluções tecnológicas que viabilizam juridicamente o uso do documento eletrônico.

1.5 Organização do Texto

O capítulo 2 apresenta uma explicação geral do fundamento básico da criptografia, bem como as diversas aplicações relacionadas que se fazem necessárias para entendimento de assuntos descritos em capítulos posteriores.

A definição de documento sob o ponto de vista jurídico; as principais características, vantagens e desvantagens das formas existentes de documento (papel e eletrônica); o enquadramento do documento eletrônico sob os aspectos legais; levantamento dos requisitos necessários e métodos para garantia destes na forma eletrônica, estão descritas no capítulo 3.

Conseguinte, o capítulo 4, refere-se aos principais aspectos a serem analisados com a introdução da validação jurídica da assinatura digital, tais como, leis existentes, migração entre as formas de documentos existentes, sistema cartorário brasileiro e tempo de validade da assinatura digital.

No capítulo 5 são apresentados o padrão de codificação **ASN.1** e os padrões **XML** para assinaturas digitais.

O capítulo 6 descreve a proposta de Infra-estrutura de armazenamento e recuperação segura de documentos eletrônicos por longo prazo e as autoridades integrantes. São apresentadas o método de funcionamento, organização e segurança da IARSDE.

O último capítulo, 7, as considerações finais da dissertação, onde são apresentados os resultados obtidos e sugestões de trabalhos futuros.

Capítulo 2

Fundamentos de Criptografia

2.1 Introdução

O entendimento da obtenção de diversos atributos jurídicos dos documentos eletrônicos requer a compreensão de conceitos de criptografia e técnicas criptográficas. Este capítulo tem como objetivo apresentar explicações relacionadas ao fundamento básico da criptografia e suas aplicações, como a assinatura digital, um item essencial na proposta de dissertação.

A definição do termo criptografia é apresentado na seção 2.2. Em 2.3 e 2.4 são apresentados dois esquemas de algoritmos criptográficos baseados em chave: simétrico e assimétrico, os quais podem ser utilizados para garantir a confidencialidade, autoria e integridade das informações. A seção 2.5 descreve o funcionamento de uma função de hash, componente da assinatura digital que garante a integridade dos dados. A seção seguinte 2.6, descreve o certificado digital , identificador do signatário em uma assinatura digital; e esta é explicada na seção 2.7,onde é apresentado um exemplo numérico de um algoritmo criptográfico.

A seção 2.8 apresenta dois esquemas para realização de assinatura digitais: direita e arbitrada. Na última seção são apresentados diversos tipos de hardwares disponíveis para auxiliar na tarefa de realização da assinatura digital.

2.2 Criptografia

A palavra criptografia tem origem grega, (kriptos: escondido, oculto e grifo: grafia) e define a ciência de escrever em códigos.

A criptografia é um estudo de técnicas matemáticas relacionadas a aspectos de segurança da informação, que busca prover serviços de:[SCH 95]

- **Confidencialidade:** garantia do sigilo da informação, de forma que mesmo que um indivíduo obtenha acesso a uma informação que não seja autorizado não consiga interpretá-la.

- **Integridade dos dados:** relaciona-se com a garantia de que os dados sejam suscetíveis a verificação e detecção da manipulação de dados em um documento.

- **Autenticação:** são meios de comprovação de identificação de uma entidade ou indivíduo.

- **Não-repudiação:** refere-se ao fato das partes não poderem negar a ocorrência de uma ação previamente realizada.

Os primeiros esquemas criptográficos eram baseados somente no sigilo do algoritmo criptográfico, como a cifra de deslocamento [STI 95]. O conhecimento do algoritmo resultava na obtenção das informações. Na criptografia moderna, chaves são utilizadas em conjunto com algoritmos para garantir maior a segurança das informações [STA 99].

A chave é uma cadeia aleatória de bits utilizada em conjunto com um algoritmo. Cada chave distinta faz com que o algoritmo trabalhe de forma ligeiramente diferente.A eficiência das chaves está ligada a sua confidencialidade, assim como ocorre com as senhas.

A avaliação da segurança de algoritmos está no grau de dificuldade de conseguir obter as informações de um texto submetido a um algoritmo criptográfico sem o conhecimento da chave utilizada.

As tentativas de quebrar-se os códigos de algoritmos são chamados de ataques. Os ataques podem ser realizados pelo método de força bruta e técnicas de criptoanálise.

Nos ataques de força bruta são feitas tentativas submetendo cada possibilidades de chave, uma após a outra. Desta forma, a confiabilidade do algoritmo se deve principalmente ao tamanho da chave.

As técnicas de criptoanálise, baseiam-se no comportamento do algoritmo e buscam encontrar brechas na sua estrutura, afim de conseguir quebrar o algoritmo em um tempo menor que o ataque de força bruta.

Devido ao fato da maior parte do emprego da criptografia atualmente fazer uso de algoritmos criptográficos baseados em chave, as seções seguintes explicam o funciomento e as aplicações dos algoritmos de chave simétrica e assimétrica.

2.3 Algoritmos de Chave Simétrica

Este método de criptografia utiliza uma única chave para cifrar e decifrar os dados.

Quando dois usuários desejam comunicar-se utilizando criptografia simétrica, com a finalidade de trocar de mensagens de forma confidencial, ambos devem compartilhar uma chave. Essa chave é previamente trocada entre os comunicantes, seja pessoalmente ou através de um canal de comunicação seguro.

Para enviar o texto de forma oculta, o remetente submete o documento ao algoritmo criptográfico e utiliza a chave que compartilha com o destinatário. O documento pode trafegar por um meio inseguro sem que possa ser lido, pois suas informações encontram-se embaralhadas, e somente quem conhece a chave utilizada no processo de ciframento consegue decifrar o texto oculto e obter o texto aberto, ou seja um texto legível. A figura 2.1 ilustra este processo.

Apesar de sua simplicidade, existem alguns problemas na criptografia simétrica:

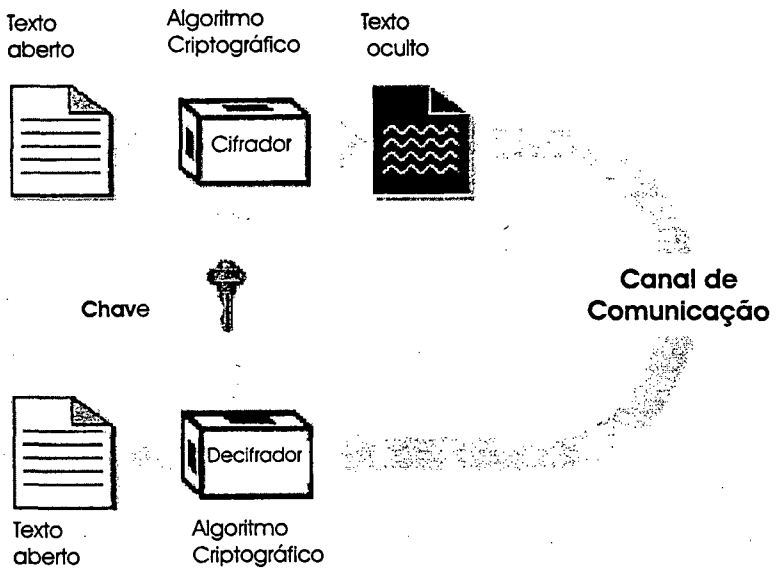

Figura 2.1: Algoritmo de chave simétrica: O processo de cifragem e decifragem dos dados utiliza apenas uma chave.

- Para cada par de indivíduos que queiram comunicar-se de forma segura, é necessário uma chave. Para uma rede de n usuários são necessárias a ordem de $n(n-1)/2$ chaves, um fator dificultador para a gerência das chaves;
- A chave deve ser trocada entre as partes e armazenada de forma segura, o que nem sempre é fácil de ser garantido;
- A criptografia simétrica não garante a identidade de quem enviou ou recebeu a mensagem.

2.4 Algoritmo de Chave Assimétrica

O conceito de criptografia de chave assimétrica foi introduzido por Whitfield Diffie e Martin Hellman [DIF 76]. A criptografia assimétrica, também chamada de chave pública envolve o uso de duas chaves distintas: a chave privada (KR) e a chave pública (KU). Neste método a chave pública é disponibilizada, tornada acessível a qualquer usuário que deseje manter comunicação com o possuidor da chave privada, sem que

haja quebra na segurança do sistema. Dessa forma cada usuário tem uma chave de cifra-mento, de conhecimento público, e outra de deciframento, secreta [GAR 97b].

A geração de um par de chaves pública/privada possui uma forte ligação matemática que garante que uma execute a operação inversa proporcionada pela outra, ou seja, se uma chave foi utilizada para cifrar um texto, somente a outra será capaz de decifrar este texto.

A grande vantagem deste método é permitir que qualquer um possa enviar uma mensagem secreta, utilizando apenas a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como é feito no modelo simétrico. A eficiência deste esquema é garantida enquanto a chave privada estiver segura. Caso contrário, quem possuir acesso à chave privada terá acesso às mensagens e também poderá personalizar o proprietário da chave.

O esquema do algoritmo de chave assimétrica pode ser utilizado para garantir tanto autenticidade quanto confidencialidade.

A confidencialidade é obtida através da utilização do algoritmo de criptografia assimétrico em conjunto com a chave pública do destinatário. Como somente o destinatário conhece a chave privada correspondente poderá decifrar a mensagem, como mostra figura 2.2.

A autenticidade garante a autoria das mensagens. Isto é alcançado com o emprego do documento ao algoritmo criptográfico, juntamente com a chave privada do remetente. Como somente o signatário deve ter conhecimento da chave privada, somente ele poderia ter gerado aquele documento.

Um dos algoritmos de chave assimétrica mais conhecidos é o RSA.

2.4.1 RSA

O RSA [RIV 78] proposto por Ron Rivest, Adi Shamir e Len Adleman em 1977 no MIT. É provavelmente, o algoritmo de chave pública mais utilizado, e uma das mais poderosas formas de criptografia de chave pública conhecidas até o hoje.

A premissa do RSA está na dificuldade de fatorar a multiplicação de

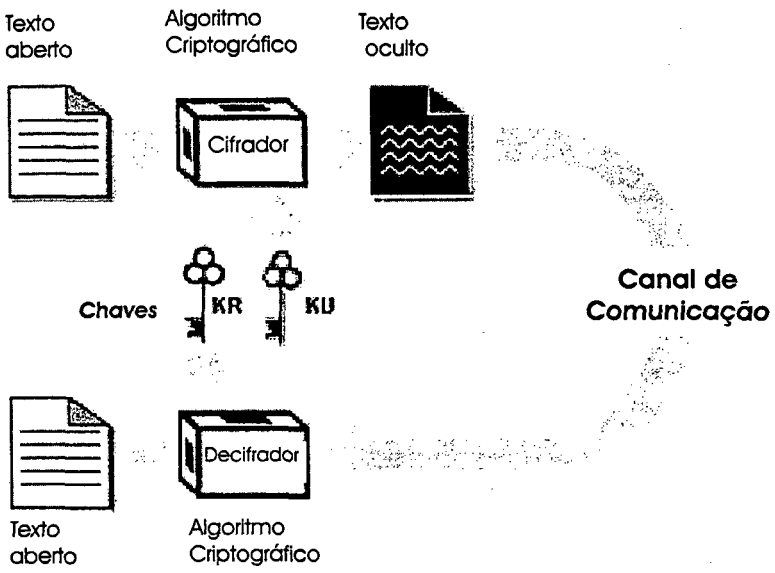

Figura 2.2: Algoritmo de chave assimétrica: Através do emprego do par de chaves pública/privada, este algoritmo provê confidencialidade e autoria do conteúdo do documento.

números primos muitos grandes, pois é fácil multiplicar dois números primos para obter um terceiro número, mas é muito difícil recuperar os dois primos a partir de um terceiro número gerado [COU 97].

Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto. Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Esses números deverão ser grandes o suficiente de forma que não exista poder computacional que possa descobri-los em tempo hábil.

Antes da utilização do algoritmo é necessário realizar previamente a geração do par de chaves (pública/privada). O passos para a geração do par chave no RSA são:

1. Selecionar p e q , ambos números primos

2. Calcular $n = p * q$

3. Calcular ϕ(n) = (p - 1)(q - 1) [totient/ de Euler]

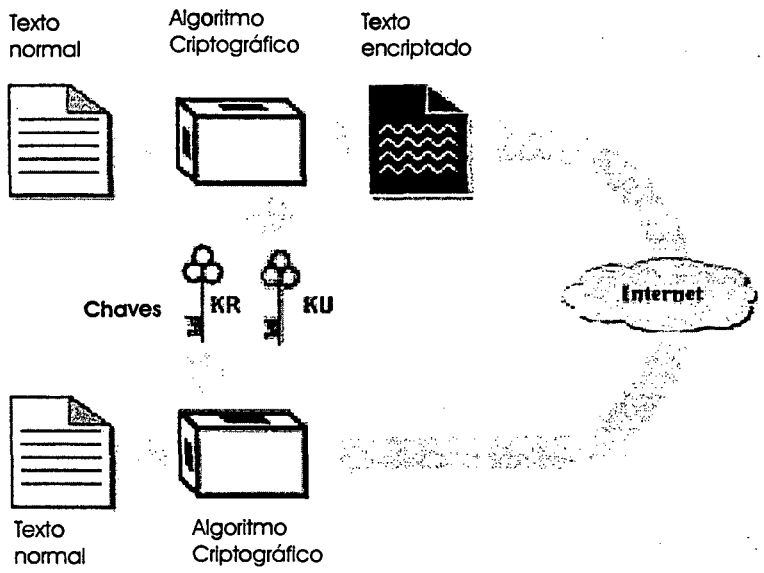

Figura 2.3: Algoritmo de chave assimétrica: Garantindo confidencialidade do conteúdo do documento

4. Selecionar inteiro e , primo relativo a ϕ(n)

5. Calcular $d = e^{-1}$ mod ϕ(n) [ou de = 1 mod ϕ(n)]

As chaves são KU = {e, n} e KR = {d, n}.

Com as chaves geradas é possível cifrar e decifrar documentos utilizando o algoritmo do RSA. A cifragem de um documento M, gerando o texto cifrado C é:

$C = M^e$ mod n

A operação inversa, a decifragem é:

$M = C^d mod n = (M^e)^d mod n = M^{ed}$ mod n

Um exemplo numérico do funcionamento do RSA, desde a geração de chaves até o processo de ciframento da mensagem é apresentado na figura 2.4

2.5 Função resumo

As funções resumo ou hash, possuem diferentes denominações: message digest, função compressora, código de detecção de manipulação, entre outras. Essas

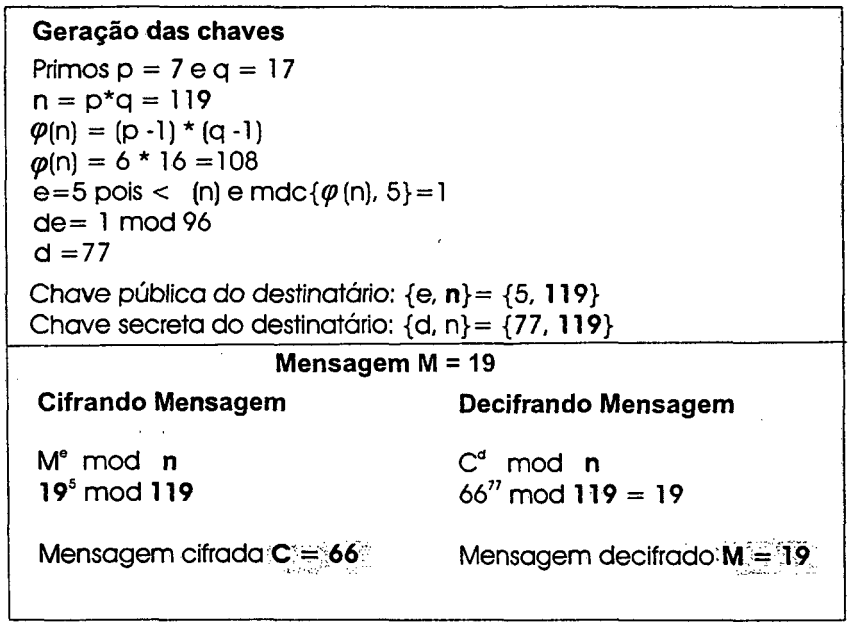

Figura 2.4: Exemplo numérico do RSA

funções são one-way, ou seja, são fáceis de computar, porém é computacionalmente difícil de obter a inversa do valor gerado a partir dele.

O produto de uma função resumo funciona como uma impressão digital de uma mensagem. A partir de uma cadeia de bits de tamanho variável é gerado uma outra de tamanho fixo: o digest ou hash. O fator que garante a segurança da função está relacionado com a independência do valor de entrada com o valor gerado como saída. Qualquer alteração da cadeia de bits original, deve gerar uma alteração significativa no valor do "hash"correspondente.

O algoritmo da função hash deve satisfazer algumas características de implementação: direção única, onde dado o resumo da mensagem, seja computacionalmente inviável encontrar a mensagem de origem; forte resistência a colisão, de forma a ser impraticável encontrar duas mensagens diferentes com o mesmo resumo e finalmente fraca resistência a colisão, que deve garantir a impossibilidade de se encontrar um par de mensagens coerentes, tal que o resumo seja igual. Dessa forma a geração do resumo, garante a integridade do documento [SAN 97].

2.6 Certificado Digital

Um certificado digital é uma coleção de informações para que uma assinatura digital seja firmada por alguma autoridade confiável e reconhecida por uma comunidade de usuários de certificado [FOR 97].

Uma analogia ao documento papel, o certificado digital seria correspondente a cédula de identidade, emitida por um órgão confiável (Secretária de Segurança Pública do Estado emissor), pois a confiança depositada em um certificado digital está na confiabilidade no órgão emissor, ou seja, na Autoridade Certificadora.

A quantidade de níveis de segurança de um certificado digital e suas especificações variam de acordo com a AC emissora. Uma AC pode definir diferentes níveis de segurança, que podem variar em função do grau de inviolabilidade, tecnologia de cifragem e modo de gestão da informação associadas aos certificados. Um exemplo da definição dos níveis é: o nível 1 garante o nível mínimo de segurança - não se verifica a identidade do utilizador, mas apenas a existência da conta de e-mail. Os certificados de nível 2, confiabilidade intermediária, sua emissão exige o recebimento de comprovantes de identidade e residência. E um certificado de nível 3, considerado de segurança máxima, implica o reconhecimento presencial do utilizador na sua identificação para emissão do certificado.

Os primeiros passos do ciclo de vida de um certificado digital constitui-se do processo de identificação do solicitante perante a AC que irá emitir o certificado digital. Esta possui normas para realizar a autenticação do solicitante. Se as condições forem atendidas, os dados são validados.

Após a fase de autenticação, a AC emite e entrega a Identidade Digital ao solicitante.

Este certificado possui campos que informam o seu tempo de utilização. Normalmente este prazo é de um ou dois anos. Após este período o proprietário do certificado não deverá mais fazer uso, pois este passará a não ter mais préstimo no sentido de realizar novas autenticações. Porém as autenticações realizadas anteriormente, no intervalo de tempo de validade do certificado permanecerão válidas caso exista formas que

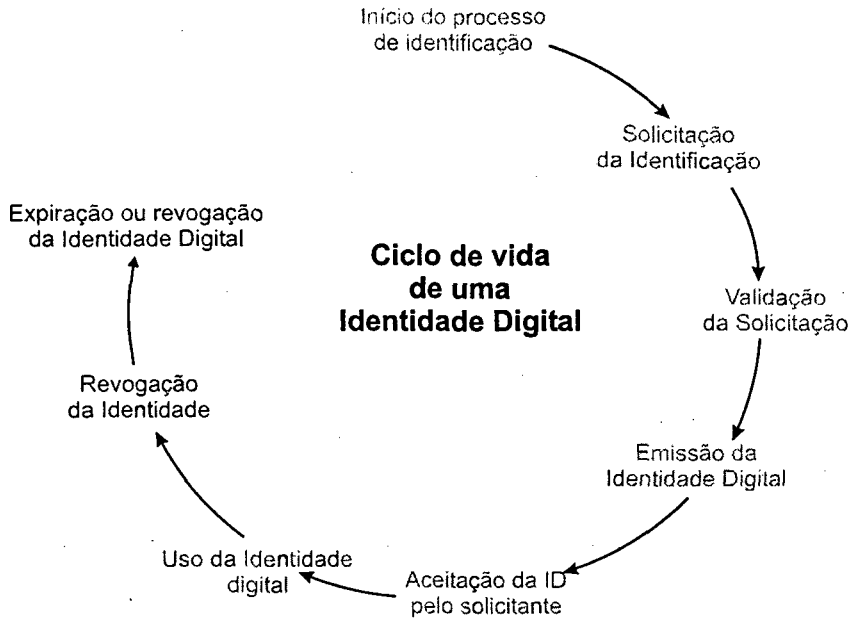

Figura 2.5: Fases do Ciclo de Vida do Certificado Digital

possibilitem a verificação do tempo da realização.

O tempo de validade também pode ser reduzido caso o proprietário solicite a revogação do certificado. Neste caso a AC incluirá este certificado nas listas de revogados, e a partir deste momento este deixa de ser válido nas autenticações .

O certificado possui um ciclo de vida associado, que vai desde o início do processo de identificação, até a expiração ou revogação, assim, todo certificado tem um prazo máximo de validade associado.

2.7 Assinatura Digital

A assinatura digital é uma aplicação da técnica de criptografia assimétrica, a qual envolve o uso de um par de chaves: chave privada, a qual serve para assinar o documento; e a chave pública, utilizada para verificar a assinatura, como apresenta o esquema da figura 2.3. Porém, a aplicação isolada desta técnica não garante a integridade do documento, então a assinatura digital faz uso conjuntamente das funções resumo.

A figura 2.6 mostra as etapas do processo de assinatura: inicialmente o signatário utiliza um algoritmo para realizar a operação de resumo dos dados do documento, através da função hash. Em seguida a chave privada é empregada na cifragem desse resumo e enviada ao destinatário junto com o documento.

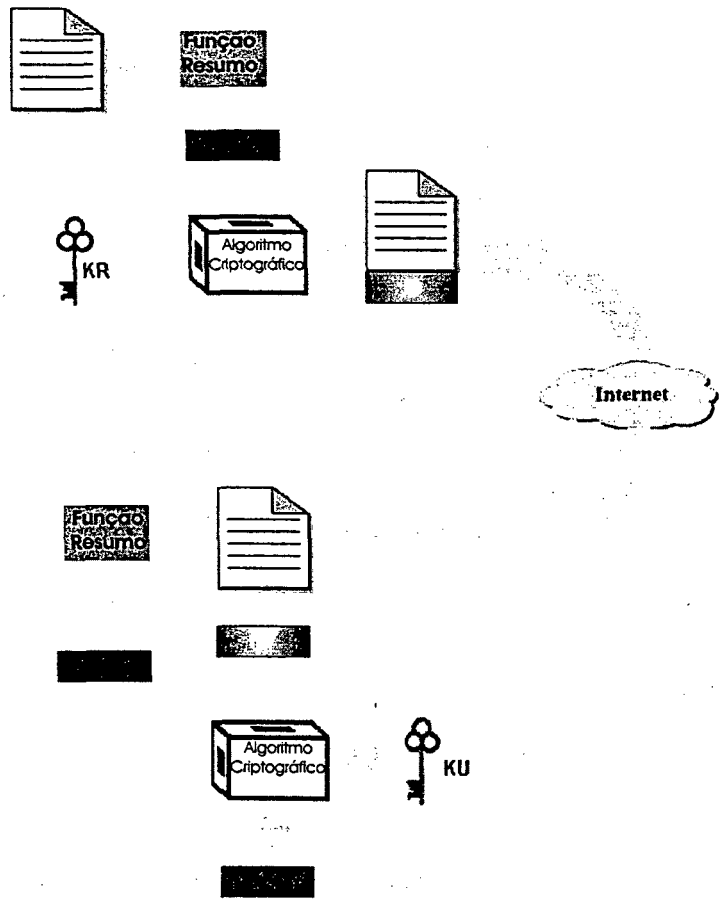

Figura 2.6: Assinatura Digital: A função de resumo juntamente com o algoritmo criptográfico de chave assimétrica garantem a integridade e autoria do documento, ou seja a assinatura digital.

A conferência da assinatura é dada através da comparação do decifra-mento do hash recebido com a chave pública e do resultado gerado da submissão do documento recebido à mesma função de hash utilizado para gerar a assinatura.

Se os valores forem iguais a autoria e integridade do documento são

certificadas.

A integridade dos dados é garantida através do resumo do documento, explicado na seção 2.5. Como o processo de verificação compara os valores do hash do documento recebido com o valor do hash do documento enviado, qualquer alteração ou tentativa de substituição do documento pode ser constatada.

No processo de geração da assinatura o hash é cifrado com a chave privada do signatário, que somente ele conhece. Isto garante a assinatura digital.

Como visto na seção 2.5, como o valor do resumo é dependente dos valores de entrada, ou seja, os dados do documento, cada resumo gerado é diferente para diferentes documentos. Como as assinaturas digitais são calculadas com relação ao hash resultante, cada assinatura digital será diferente para um mesmo signatário, diferentemente das assinaturas manuscritas nos documentos papel no qual as assinaturas apresentam pouca variação na sua forma.

O DSS (Digital Signature Standard) proposto pelo NIST em 1991, foi padronizado para geração e verificação de assinaturas digitais[NIS 94]. O DSS faz uso do hash SHA (Secure Hash Standard)[NIS 93], e apresenta uma nova técnica de assinatura digital, o DSA (Digital Signature Algorithm). O DSS é um sistema de chave pública embora tenha como única função executar assinatura digital. Não pode ser usado para cifragem ou troca de chaves. O DSA também é baseado na dificuldade do cálculo de logaritmos discretos utilizando-se esquemas do ElGamal.

O DSS apresenta algumas desvantagens em relação ao método do RSA:

- Expansão da mensagem: o tamanho dos dados praticamente dobra depois de cifrado.
- Força da assinatura: por questões de padronização do DSS, o limite do tamanho das chaves DSS é 1024 enquanto as chaves do RSA podem ter qualquer tamanho, sendo muito comum o uso de 1024 a 4096 bits, variando conforme a implementação
- Intensidade Computacional: o DSS exige mais tempo de processador que o RSA. Essa diferença é bastante evidente em dispositivos como smartcards/chips embutidos.

Este é um padrão de assinatura digital que encontra-se inadequado para os dias de hoje, principalmente pela limitação imposta com relação ao tamanho das chave.

2.8 Formas de Assinatura Digital

A confiabilidade da assinatura digital depende de um fator de confiança associado para que seja possível efetuar a autenticidade do documento. Existem duas formas de assinatura digital: a direta e a indireta.

Assinatura Direta

A assinatura direta envolve somente a comunicação entre as partes, destino e origem, ilustrada na figura 2.7. Esta esquema supõe que o destinatário conhece a chave pública da origem [STA 99].

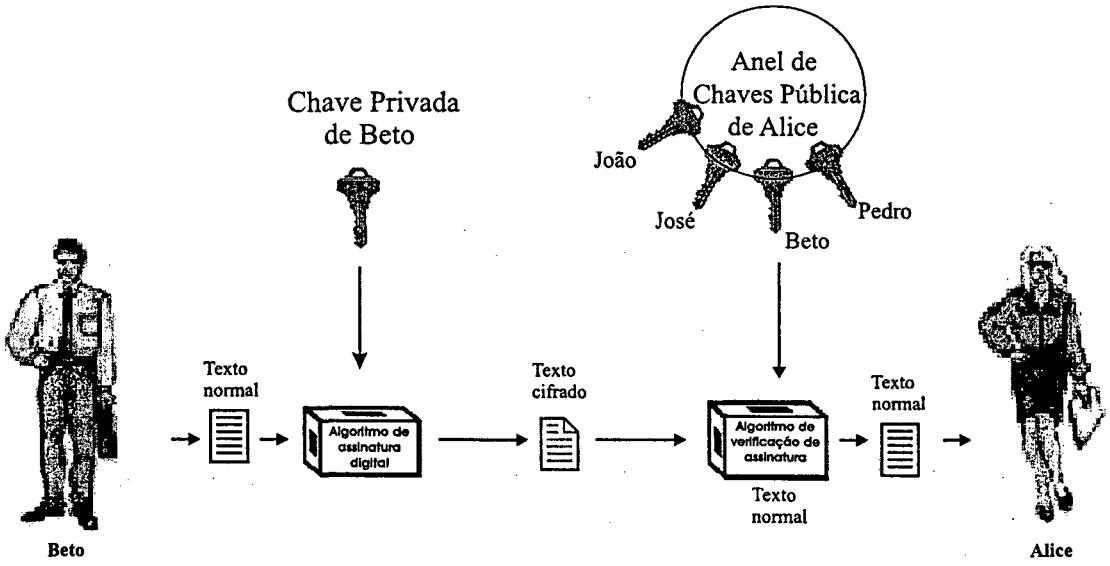

Figura 2.7: Assinatura Direta: Assinatura digital envolvendo apenas os elementos participantes.

Uma assinatura pode ser formada pela cifragem da mensagem inteira ou do resumo da mensagem utilizando a chave privada do signatário.

Os esquemas de assinatura direta possuem como ponto frágil, a dependência da segurança da chave privada para seu êxito, pois no caso do comprometi-

mento ou compartilhamento desta, as assinaturas podem ser personalizadas.

Assinatura Indireta

A assinatura indireta, também conhecida com assinatura arbitrada, envolve um terceiro elemento presente na comunicação entre a origem e o destinatário para a realização da assinatura, denominado árbitro ou juiz, conforme figura 2.8.

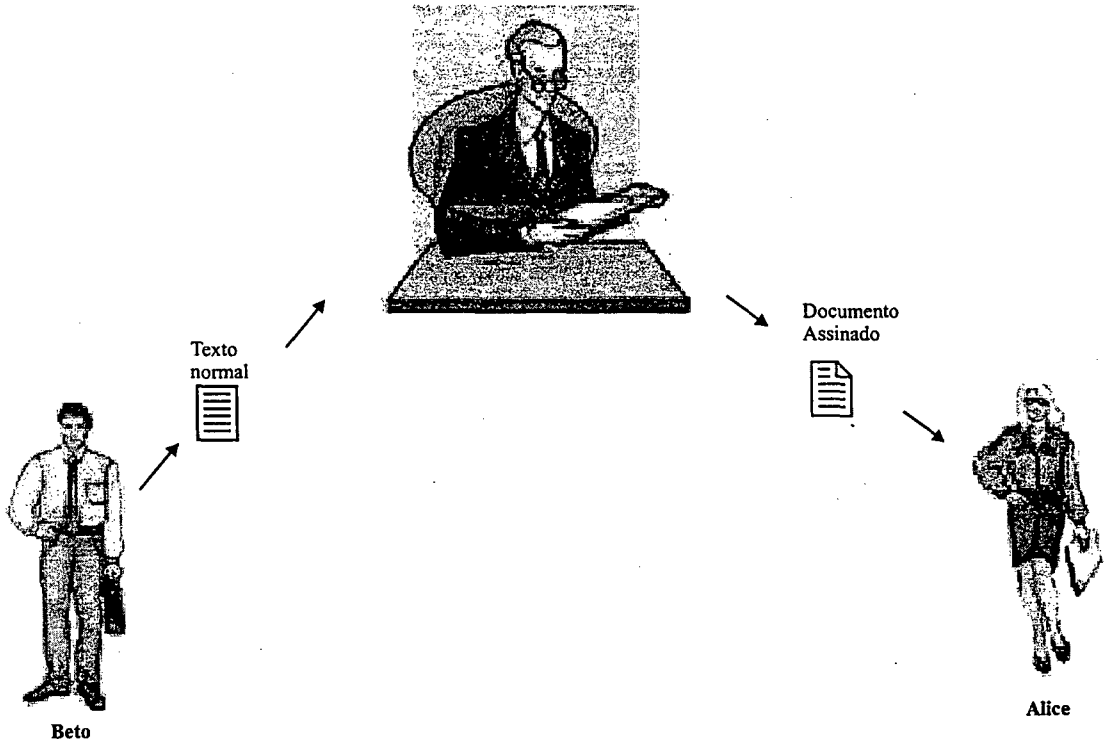

Figura 2.8: Assinatura Arbitrada

Em geral o esquema de assinatura indireta tem como operaçõs os seguintes passos: toda mensagem assinada por um emissor X para um receptor Y vai primeiro para um árbitro A, que sujeita a mensagem a assinatura desta a vários testes para verificar a origem e conteúdo. A mensagem é então datada e enviada para Y com a indicação que foi verificada pelo árbitro [STA 99].

Esse esquema não necessita necessariamente utilizar de algoritmos de criptografia assimétrica, pois a confiabilidade entre os elementos e o árbitro pode ser dada através do compartilhamento de chaves simétricas.

Ambas as formas de garantir a assinatura digital possuem pontos fortes e fraquezas, porém no esquema arbitrado, a garantia da assinatura é totalmente dependente da confiança no árbitro, não sendo considerada uma solução muito adequada, uma vez que a confiabilidade da assinatura deixa de estar associada ao signatário.

Nos capítulos que seguem todas as assinaturas digitais citadas devem ser consideradas baseadas na assinatura direta.

2.8.1 Hardware

A segurança dos esquemas de assinatura digital pode ser incrementada com a utilização de hardwares específicos, sejam eles para auxiliar na confidencialidade da chave privada ou para prover formas de autenticação baseada em dados biométricos.

O smartcard é uma forma de implementar maior segurança na autenticação. É um cartão plástico do tamanho de um cartão de banco ou cartão de crédito normal, porém com um pequeno microchip cravado em sua superfície que armazena, processa e troca informações com outros sistemas. Sua principal função é armazenar e processar informações de forma segura e permitir que essa informação apenas seja acessada ou alterada por pessoas autorizadas. Isso permite que o smartcard seja usado para informações sigilosas, ou mesmo processar pequenas quantidades de informação para verificar se são válidas ou não, como por exemplo senhas de acesso.

O smartcard realiza o procedimento necessário para autenticação sem mostrar a informação protegida. Essas informações são protegidas através de processos de criptografia, com chaves e senhas de acesso. Além disso, existem cartões com sistemas operacionais que exigem uma série de procedimentos para validação e identificação de quem está solicitando as informações.

Além do smartcard, existem diversos hardwares disponíveis que auxiliam no processo de autenticação, resultando em um maior grau de segurança. A maior parte destes equipamentos são utilizados juntamente com software de reconhecimento a partir de dados biométricos.

Existem várias formas de sistemas biométricos. Para implantá-los são

necessários equipamentos especiais e softwares que tratem os dados capturados. De forma generalizada, todos funcionam sobre os mesmos princípios, mas, para cada caso, o hardware e o software devem ser otimizados para o elemento biométrico adotado. Os principais métodos e recursos necessários são [GOY 00]:

- impressão digital: O método requer um scanner capaz de capturar imagens com um bom grau de precisão dos traços que definem a impressão dos dedos. Os *scanners* para captura da impressão digital possuem tamanho relativamente reduzido. Alguns modelos são independentes e podem ser anexados ao teclado, monitor ou gabinete do computador. Outros já possuem o mecanismo acoplado a dispositivos como mouse, teclado e terminais;

- reconhecimento da face: é necessário uma pequena câmera que é usada para a captura da imagem do rosto, possibilitando o registro de vários pontos delimitadores na face, capazes de definir proporções, distâncias, tamanhos e formas de cada elemento do rosto, como olhos, nariz, queixo, maçãs do rosto, orelhas, etc;

- identificação pela íris: para implementar esse tipo de sistema biométrico, é necessária uma câmera para a captura da imagem, a qual pode ser monocromática, pois as cores não são significativas para a identificação.

- assinatura manuscrita: são necessários uma pequena prancheta digitalizadora e uma caneta especial. Esses dispositivos normalmente permitem a captura da pressão, velocidade e posição da caneta, definindo o comportamento da escrita e o transcreve em um modelo matemático que identifica a assinatura e o usuário respectivo.

2.9 Conclusão

Este capítulo apresentou uma revisão bibliográfica de componentes criptográficos necessários para tornar possível o entendimento de itens essencias desta monografia. O principal deles é a assinatura digital. Dentre os elementos abordados relacionados a assinatura digital estão o certificado digital e a função resumo. Os processos que

envolvem estas operações relacionam-se com o estudo do levantamento dos requisitos tecnológicos do documento eletrônico discutidos no próximo capítulo.

Capítulo 3

Documento

3.1 Introdução

A utilização de transações eletrônicas na Internet tem crescido muito em relação as formas de transações tradicionais, seja devido ao crescimento do número daqueles que utilizam a Internet ou pelo aumento da diversificação de atividades que esta tem proporcionado.

Entre os pontos levantados por aqueles que utilizam serviços disponíveis na Internet para realização de negócios, trocas de informações valiosas, estabelecimento de relações de diversos níveis, a segurança é o item que tem sido dada maior atenção, pois se inexistir mecanismos que garantam a validade de um documento eletrônico, as relações entre as entidades que trocam estes documentos tornam-se frágeis. Como por exemplo, um contrato, pode ser alterado maliciosamente e comprometer as partes envolvidas. Os mecanismos que garantem esta validade são a integridade, a confiabilidade e o não repúdio.

No mundo real[1] a ocorrência de assinaturas falsificadas e documentos forjados, não deixa de existir e portanto estes fatores não são problemas associados apenas ao mundo virtual. Porém no mundo real, já existem diversos sistemas de proteção para

[1]Neste trabalho o termo *mundo real* é utilizado apenas para fazer referência a um ambiente de documentos no formato papel.

diferentes tipos de fraudes nos documentos tradicionais, os quais são amparados pelas legislações civil e penal, que dispõem de normas inibidoras e repressoras em prol da sociedade.

No mundo virtual[2] as definições de documento eletrônico, assinatura digital e sua validade jurídica são assuntos que ainda encontram-se em estudo e discussão, para obter-se uma forma segura e abrangente equivalente ao existente no mundo real nas novas relações eletrônicas de cunho comercial e social, que estes elementos propiciaram.

O estudo do enquadramento do documento eletrônico na definição dos documentos e seus requisitos, analisando suas fragilidades e carências em relação ao documento papel tem grande importância para a elaboração da infra-estrutura proposta no capítulo 6.

Na seção 3.2 são expostas as principais características dos documentos na forma papel e eletrônica. A seção 3.3, traz a definição de um documento sobre a visão jurídica e como o documento eletrônico se enquadra nesta definição. A seção 3.4 descreve os atributos que um documento deve possuir, as formas para provê-los e as fragilidades e vantagens que cada uma apresenta.

3.2 Documento papel x documento eletrônico

A popularização dos computadores na década de 1980, gerou muitas perspectivas em relação ao fim do documento papel. Paradoxalmente, se imaginava que a automatização de processos e o surgimento de documentos eletrônicos reduziriam o número de documentos papéis. Todavia a facilidade de tratamento de dados e o surgimento de equipamentos de impressão, trouxeram na realidade um aumento no volume de documentos papéis.

Porém, obter dados é relativamente fácil comparado à obtenção de informações. As informações são geradas pelo tratamento de dados. Um exemplo de fácil visualização é a entrega de declaração de imposto de renda, onde milhares de formulários

[2]O termo *mundo virtual* faz referência ao tratamento de documentos no formato eletrônico.

são entregues à Receita Federal, apostados com um grande volume de dados brutos. Somente após a análise de dados são extraídas informações úteis e relevantes.

Os meios computacionais existentes são mais eficazes tanto no tratamento dos dados como na localização da informação. Em decorrência disto, os documentos papel têm perdido espaço para documentos eletrônicos não somente em razão dessas dificuldades de manuseio e tratamento da informação, mas principalmente pelo alto custo que estas operações demandam.

Pesquisas realizadas em 1993[CEN 98], revelaram que o custo de armazenamento de documentos papel, deve elevar-se com tempo, enquanto a forma eletrônica deve apresentar um sentindo inverso, ou seja, cada vez mais baratos.

Documentos eletrônicos têm ganho emprego em diferentes atividades, tais como transações comerciais, fechamento de acordos e contratos, não somente pelos fatores anteriormente comentados, mas principalmente pela agilidade que este traz à circulação das informações. Além da diversidade de uso, os documentos eletrônicos também podem apresentar vantagem em relação ao documento papel, em alguns aspectos:

- Grandes volumes documentais na forma papel, podem necessitar de grande espaço físico para armazenamento. A conversão para a forma digital, resolve este problema, pois a manutenção destes dados podem ser feitos em pequenos dispositivos, como fitas, discos rígidos, cds, dvd, etc;

- É mais fácil a gerência de dados na forma eletrônica, pois a atualização e localização dos dados normalmente é mais eficaz, rápida e precisa.

- Os documentos eletrônicos proporcionam disponibilidade de cópia a um baixo custo;

- O documento eletrônico não apresenta desgaste físico.

- o documento papel não exige a utilização de qualquer artifício para sua visualização, enquanto em um documento eletrônico se faz necessário a utilização de um software

que traduza a seqüência de bits do arquivo para uma forma que se possa verificar o conteúdo do mesmo, como mostra figura 3.1.

- o papel ainda é mais ergonômico que qualquer sistema de visualização existente para documentos eletrônicos;

- marcas, impressões, formas de alto relevo existentes em documentos papéis, que garantem controle de cópias ou origem do emissor, não podem ser facilmente transferidos para documentos eletrônicos;

- por razões culturais as pessoas e as instituições podem apresentar resistência para adotar a utilização de documentos eletrônicos.

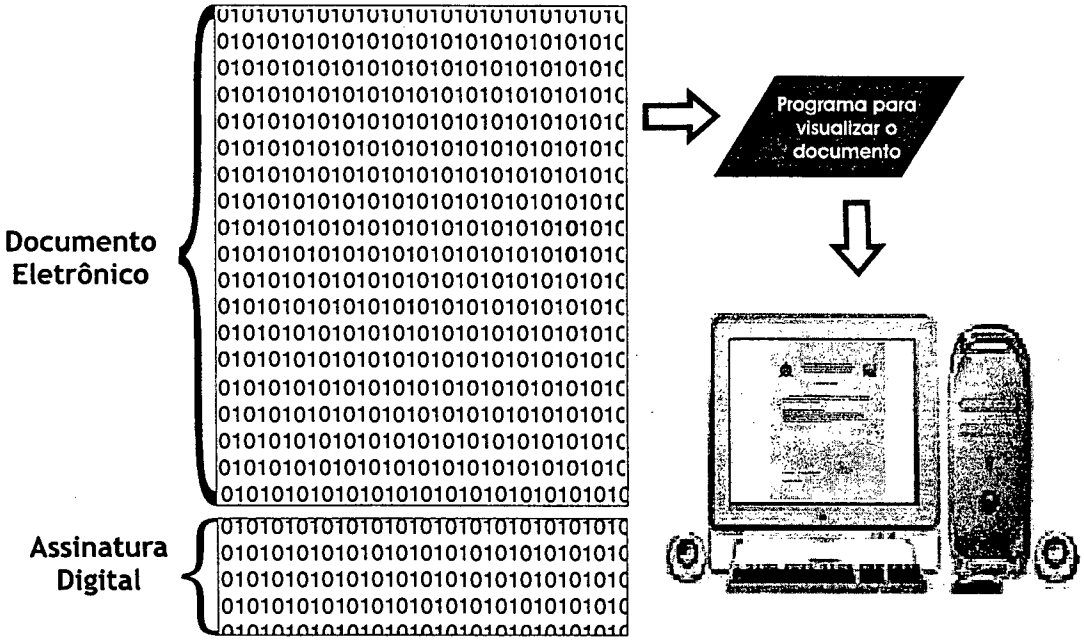

Figura 3.1: Documento Eletrônico: O Processo de visualização do documento eletrônico necessita de um programa que traduza a seqüência binária de um arquivo para uma forma visualmente compreensível.

Com base nos aspectos apresentados, acredita-se que por muito tempo ambas formas de documentos devam permanecer.

3.3 O conceito de documento

A interpretação mais usual da palavra documento é *"qualquer base de conhecimento, fixada materialmente e disposta de maneira que se possa utilizar para consulta, estudo, prova, etc"*[dH 96]

O termo "documento"na doutrina jurídica possui diversas acepções, para JOSÉ FREDERICO MARQUES, documento é a prova histórica real consistente na representação física de um fato. O elemento de convicção decorre, assim, na prova documental, da representação exterior e concreta do *factum probandum* em alguma coisa.

HUMBERTO THEODORO JÚNIOR leciona que documento *"é o resultado de uma obra humana que tenha por objetivo a fixação ou retratação material de algum acontecimento"*[JR 96]. MOACYR AMARAL SANTOS conceitua documento como sendo *"a coisa representativa de um fato e destinada a fixá-lo de modo permanente e idôneo, reproduzindo-o em juízo"*[SAN 97].

A preocupação da ligação de conceitos e definições de documento à sua materialidade, não é desprovida de fundamento, uma vez que não haveria muito sentido em registrar-se informações fielmente, se estes registros não pudessem existir fisicamente de alguma forma. Se os registros fossem apenas transitórios, desprovidos de perenidade, a informação não poderia persistir. Um exemplo que pode ser citado é a Bíblia. Se tivesse sido escrita sobre as areias do Oriente Médio, teria sido um registro efêmero e inútil para os fins que se espera. Portanto, o grau de perenidade que um documento confere ao seu conteúdo, depende do suporte material utilizado [SAN 97].

Em virtude dessa dependência da informação ao seu suporte físico, é que o documento acabou sendo concebido como coisa. Logo o documento é associado com algo tangível, palpável e imediatamente perceptível, em suas formas e significados. A associação da informação de um documento a um indissociável suporte material, trouxe a confusão do suporte, que é um mero instrumento, com o documento em si, a composição de informações.

O conceito da aposição da informação a algo material é um dos fatores mais citados em conceitos tradicionais de documento, o qual considera que ele se con-

substancia numa coisa fixada materialmente. Porém diversos doutrinadores definiram o documento como "o escrito", e não como "a coisa":

CHIOVENDA define: "*documento, em sentido amplo, é toda representação material destinada a reproduzir determinada manifestação do pensamento, como uma voz fixada duradouramente*"[CHI 69].

JULIO FABBRINI MIRABETE define documento como proveniente de doceo, ensinar, mostrar, indicar e consubstanciando-se no "*escrito que condensa graficamente o pensamento de alguém, podendo provar um fato ou realização de algum ato dotado de significação ou relevância jurídica*"[MIR 95].

Um aditivo à ótica da representatividade do fato, é a proveniência do termo "documento", originária do latim, documentum, a qual deriva de *docere*, que significa ensinar, mostrar, indicar. Isso revela a característica essencial do documento, a transmissão de informações, onde a fixação da informação, a coisa corpórea, deve ser considerada apenas como um meio para atingir um documento fim.

Isso vem a reforçar a definição de documento como uma coisa representativa de um fato, a qual o documento eletrônico se adequa perfeitamente ao conceito, pois pode constituir-se de uma seqüência de bits que pode ser interpretada por meio de softwares que possibilitam a verificação da expressão do pensamento ou vontade daquele que o formulou.

Porém deve se considerar que "*da mesma forma que os documentos físicos, o documento eletrônico não se resume em escritos: pode ser um texto escrito, como também pode ser um desenho, uma fotografia digitalizada, sons, vídeos, enfim, tudo que puder representar um fato e que esteja armazenado em um arquivo digital*"[MAR 98].

Moacyr Amaral Santos especifica os documentos, "*escritos são os em que os fatos são representados literalmente (escritura); gráficos, os em que são por outros meios gráficos, diversos da escrita (desenho, pintura, carta topográfica); plásticos, os em que a coisa é representada por meios plásticos (modelos de gesso ou madeira, miniaturas); estampados são os documentos diretos (fotografia, fonografia, cinematografia)*"[SAN 97].

Concluindo nesta linha de pensamento, os documentos não consistem apenas de palavras escritas, podendo ser composto de textos, imagens, sons ou figuras.

Sobre o mesma tema, HUMBERTO THEODORO JÚNIOR descreve: "*Em sentido lato, documento compreende não apenas os escritos, mas toda e qualquer coisa que transmita diretamente um registro físico a respeito de algum fato, como os desenhos, as fotografias, as gravações sonoras, filmes cinematográficos, etc. Mas, em sentido estrito, quando se fala da prova documental, cuida-se especificamente dos documentos escritos, que são aqueles em que o fato vem registrado através da palavra escrita, em papel ou outro material adequado.*"[JR 96].

Analisando os diferentes prismas da definição de documento, o documento eletrônico pode se encaixar nas definições da representatividade do fato.

Henrique Martins faz um comentário interessante a respeito dessa divergência do enquadramento do documento eletrônico como documento: "*O Direito tem dificuldade em adaptar-se a estes avanços tecnológicos não somente pela rapidez destes avanços, mas também pela própria natureza do ciberespaço, um lugar onde inexistem fronteiras físicas e barreiras criando problemas para a jurisdição e legalização de transações comerciais. Os maiores problemas que surgem relacionados ao Direito são: (i) a segurança nos pagamentos das práticas comerciais, (ii) a segurança nas transações em geral para assegurar um ambiente de confiança e garantir a autenticação eletrônica dos dados, a sua integridade e confidencialidade; (iii) a elaboração dos contratos no tocante à sua forma; (iv) ao momento e local de celebração dos contratos e a representação legítima; e (v) a responsabilidade civil (o não cumprimento, erros de transmissão, etc)*"[MAR 00].

"*No Brasil, o importante é a vontade, ou seja, a declaração de vontade expressamente manifestada, demonstrada por qualquer meio permitido legalmente, e seus efeitos. Neste ponto, podemos atentar para os artigos 129 [2], 136, 1289 e 1290, todos do Código Civil. A assinatura simplesmente é uma das formas de declaração. Por exemplo: se uma pessoa tem uma assinatura eletrônica e outra pessoa entra em seu micro e contrata em seu nome usando sua assinatura, não necessariamente a pessoa prejudicada (desde que prove) deva cumprir o mesmo. O que acontecerá é que ela deverá ressarcir o contratante prejudicado com perdas e danos, mas não necessariamente deve cumprir a obrigação.*

3.4 Atributos essenciais dos documentos eletrônicos

É de fundamental importância a abordagem de conceitos tecnológicos que atendam diversos requisitos implícitos na definição de documento.

Relacionado a este tema a medida provisória 2.200 trata matérias de grande importância de forma vaga, prevendo que "Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória"(art. 12) e também, "A todos é assegurado o direito de se comunicar com os órgãos públicos por meio eletrônico". Isso se torna um grande dificultador na tarefa posterior de regulamentação dos documentos eletrônicos.

Os atributos essenciais estão relacionados a autoria, integridade, aspectos temporais e não repúdio. Para cada atributo do documento eletrônico, são apresentadas técnicas ou propostas para atender essa necessidade. Aqui são analisadas as características funcionais, suas fragilidades e pontos fortes.

3.4.1 Autoria e Integridade

Com relação ao fato da necessidade de um documento estar ligado a um autor de forma passível de verificação, e a garantia da existência de métodos que gerem prognóstico de ocorrência de alteração dos dados no documento vem de encontro com os requisitos básicos para definição de um documento, como AUGUSTO T. R. MARCACINI afirma: "*Em se tratando de documento indireto - que é o tipo mais comum - necessário se faz, para emprestar-lhe força probante, que: a) tenha autoria identificável (autenticidade); b) que não possa ser alterado de modo imperceptível (integridade). Autenticidade e integridade são, portanto, os requisitos básicos que deve conter um documento para servir como prova.*"[MAR 98].

Seguindo a mesma linha de pensamento, ÉLCIO TRUJILLO ratifica as palavras de Raimondo Zagami: "*O que nos importa aqui é o valor probatório do documento - seja em que base material esteja 'inscrito' - está na dependência de que esse suporte material deva ser indelével, i.e., que não permita qualquer tipo de adulteração, deliqüescência ou cancelamento que de outra forma não possa ser percebido. Ademais,*

é necessário que haja uma imputação subjetiva segura, que permita o estabelecimento da presunção relativa de proveniência - o que tradicionalmente se verifica com a aposição da firma, uma escritura autógrafo que se presume única para cada indivíduo e que seja difícil de ser reproduzida, não seja modificável e igualmente não possa ser reutilizável quando ligada indissoluvelmente ao suporte material que a contém. É evidente a relevância jurídica da assinatura para a identificação da proveniência e paternidade do documento."[TRU 97]

Assim a análise de requisitos de segurança deve considerar dois aspectos básicos: o documento, para que assim possa ser chamado, deve prover formas de identificação do seu autor. Isso pode ser dado por meio de um sinal pessoal, denominado assinatura ou firma. Outro aspecto é a credibilidade, a qual está ligada essencialmente à sua originalidade, onde se pode verificar a integridade quanto a possíveis alterações sofridas pelo percurso do documento até seu destino.

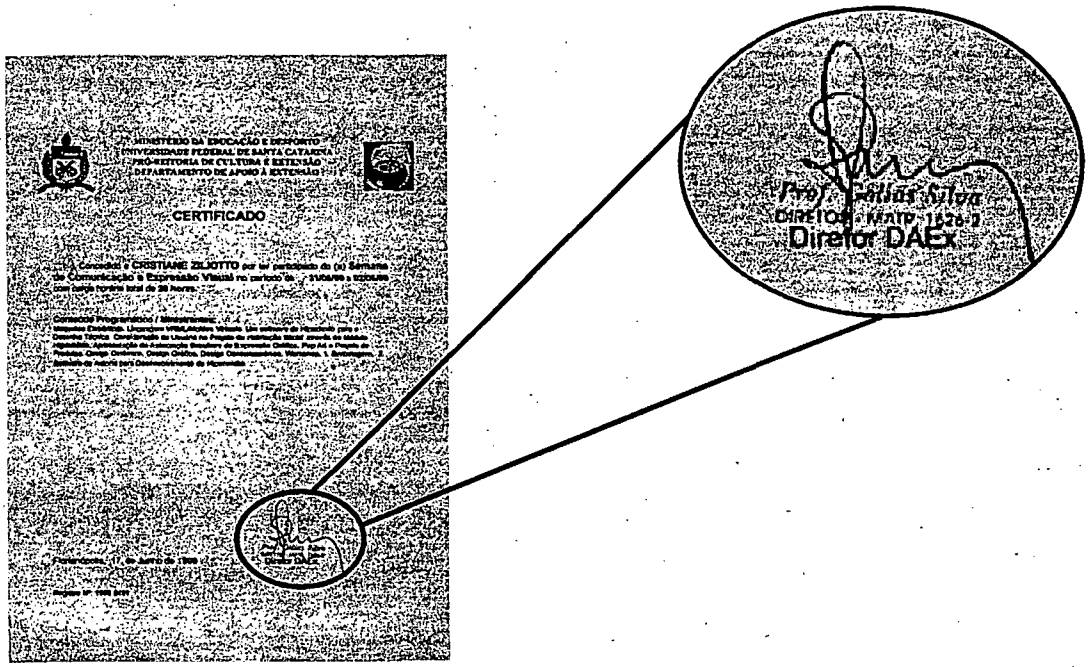

Figura 3.2: Documento Papel: A visualização da assinatura manuscrita aposta sobre o documento papel sem a necessidade de artifícios.

O primeiro item é facilmente verificado no documento papel, pois a au-

tor ao assinar o documento de forma a autenticá-lo, o faz em um algo tangível, o papel, sendo este a entidade física de ligação entre a informação impressa e a assinatura, conforme pode ser visto na figura 3.2.

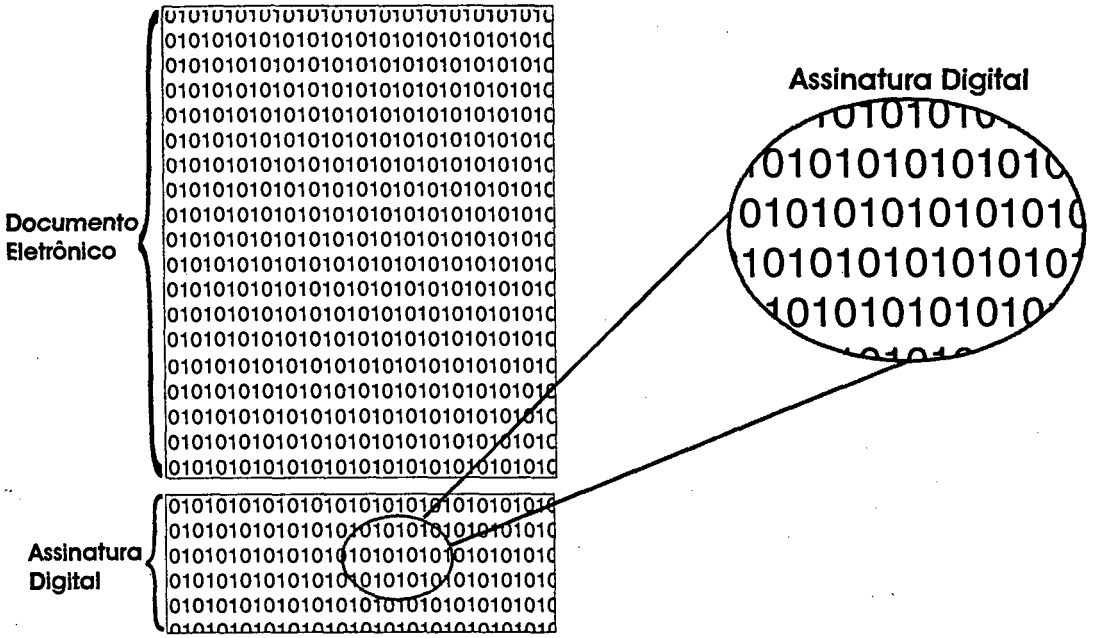

Figura 3.3: Documento Eletrônico: Documento e assinatura na forma eletrônica.

A autoria nos documentos eletrônicos, é garantida através de diversos processos realizados sobre a informação do documento que geram uma identificação única ligada ao autor, denominada assinatura digital. Entretanto, assim como o documento eletrônico apresenta-se como uma seqüência de bits (0 e 1), a assinatura possui a mesma forma (a figura 3.3 apresenta esta característica).

A assinatura digital garante não somente a autoria, mas também a integridade do documento, pois a ocorrência de qualquer alteração, por menor que seja, a assinatura não é verificada. Essa é uma vantagem apresentada sobre a assinatura escrita, uma vez aposta sobre o papel, existem formas de realizar alteração sob o documento sem que isso seja detectado. Porém a sua visualização e verificação, como o documento, também dependem de um software que realize a tradução da seqüência de bits.

Outro aspecto relevante é a autoria, que está ligada a confidencialidade

de um elemento (chave privada) do esquema de assinatura digital. Esses fatos demonstram duas relações de dependência:

- A relação da integridade do conteúdo com a confiabilidade do software. Caso o software seja malicioso, os dados do documento podem não ser reproduzidos fielmente não expressando a vontade daquele que o originou;

- Autoria com a confidencialidade da chave privada. Como a chave privada é o elemento que liga o signatário ao certificado digital (identificador do emissor), este deve mantê-lo em segredo, pois em caso de compartilhamento deste elemento é possível haver personificação do signatário.

A conferência das assinaturas tanto no documento papel como na forma eletrônica, tem como base uma identificação emitida por um órgão confiável.

A verificação da autenticidade da assinatura no documento papel pode ser feita através da comparação de um documento de identidade emitido pela Secretaria de Estado de Segurança Pública de algum estado, pois esta tem validade em todo território nacional, e constitui-se de um órgão confiável, ver figura 3.4.

No papel, o documento pode ser submetido a uma entidade cartorária e dado fé pública por um tabelião. Assim este documento é considerado válido devido a identificação dada por um órgão confiável.

Em ambas as formas, para a verificação é necessária somente a visualização, sem a necessidade de nenhum artífício.

No documento eletrônico o documento é também um certificado emitido por uma Autoridade Certificadora (AC) confiável. Porém o processo de verificação da assinatura não pode ser feita apenas visualizando a assinatura e o documento do órgão confiável.

Assim como para a visualização, é necessário um software de verificação de assinatura digifal confiável que realize operações matemáticas sobre o documento e a assinatura para constatar a validade destes, conforme mostra a figura 3.5.

Como observado, os documentos eletrônicos atendem os requisitos de

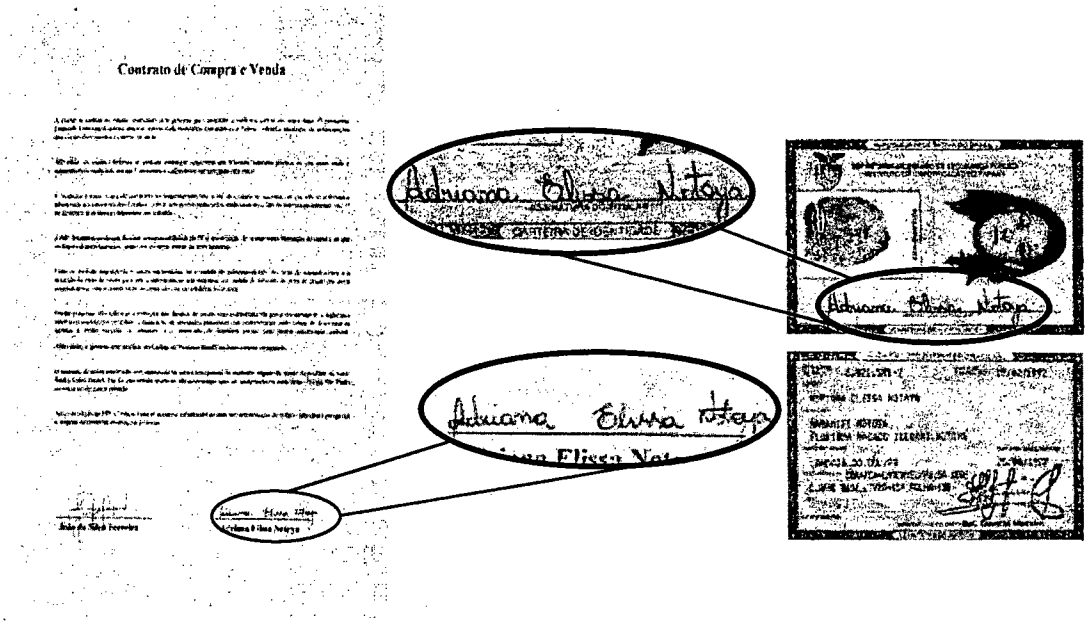

Figura 3.4: Conferência da assinatura: Verificação da assinatura aposta sobre um documento papel através de um RG, emitido por uma entidade confiável, a Secretaria de Segurança Pública.

autoria e integridade, e se fizerem uso de tecnologias eficientes e confiáveis, eles podem apresentar-se mais seguros que documentos papel.

3.4.2 Não Repúdio

Não repúdio, segundo definição de ABA Guidelines são "*evidências fortes e substanciais da identidade do signatário e da integridade da mensagem, suficiente para prevenir com sucesso que uma parte negue a origem, submissão ou entrega da mensagem e integridade do conteúdo*".

O não repúdio é um atributo de garantia que uma parte não possa negar um fato ocorrido. Assim, o não Repúdio pode ser definido como um atributo em uma comunicação onde as partes são protegidas contra a alegação de inexistência, o que representa que a figura do não repúdio está presente para produzir efeitos legais nos contratos feitos por meio eletrônico.

A diferença da autenticidade e da integridade do documento na figura do

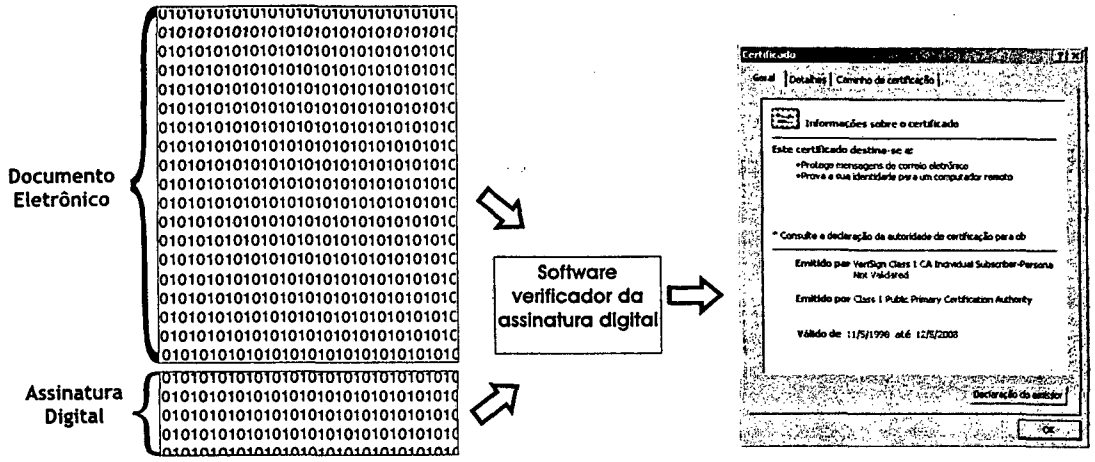

Figura 3.5: Verificação da Assinatura Digital: O processo de verificação e visualização da assinatura digital por meio do tratamento dos dados através de um software.

Não Repúdio está na capacidade de se provar a uma terceira pessoa que uma comunicação foi realizada, admitida e enviada com sucesso a outra parte, sem que seja necessária a apresentação da assinatura tradicional, como se admite no direito.

Após a assinatura digital, é necessário que haja um acordo entre os contratantes para a inclusão do Não Repúdio no negócio para que possa gerar os devidos efeitos legais. somente com estes atributos poder-se-á demonstrar e fazer valer como prova em caso de disputa judicial, demonstrando que o negócio existiu e houve aceitação [BRA 01].

Portanto, este é um atributo imprescindível que deve ser observado nos documentos eletrônicos, tanto do ponto de vista jurídico como técnico, para que se possa alcançar correspondência com os documentos formais em relação as normas de direito civil, e assim possam ser aplicadas e utilizadas da mesma forma. Para isso o documento deve conter prova de sua validade, não querendo dizer que o Não Repúdio torna o negócio definitivo do ponto de vista legal. Se no plano dos negócios fora do mundo eletrônico existe a possibilidade da desistência e do pagamento de multas por inadimplência e até mesmo a possibilidade do desfazimento do contrato, isso também poderá ocorrer nas transações on line. O que o Não Repúdio traz de novo é uma forma de seguro contra a alegação de que o negócio não foi realizado e existência de provas em caso de disputa

judicial, mantendo a cláusula da garantia para as partes.

A comunicação bilateral ou multilateral envolve dois tipos primitivos de partes: remetente e receptor. Correspondentemente, não-repúdio pode ser subdividido em duas partes primárias: não repudiação da origem e não repudiação da entrega [FOR 97].

3.4.2.1 Não repudiação da origem

A não repudiação da origem fornece provas suficientes para resolver as disputas abaixo, de modo a proteger os receptores dos casos a seguir:

- o receptor alega que recebeu uma mensagem, mas a parte identificada como remetente alega não ter enviado nenhuma mensagem;
- o receptor alega ter recebido uma mensagem diferente da que o remetente afirma ter enviado;
- o receptor alega o recebimento de uma mensagem originada em uma data e tempo específico, mas a parte identificada alega ter enviado essa mensagem em particular nesse tempo.

3.4.2.2 Não repudiação de entrega

Não repudiação de entrega previne ou resolve desacordos em relação ao recebimento de dados, tempo de entrega, ou ambos, ou seja, protege o remetente provendo provas suficientes para solucionar as seguintes disputas:

- o remetente afirma ter enviado uma mensagem, mas a parte identificada como receptora alega não ter recebido;
- o remetente afirma ter enviado uma mensagem diferente da que o receptor afirma ter recebido;
- o remetente afirma ter enviado uma mensagem particular em uma data e tempo específico, mas o receptor alega não ter recebido a mensagem no mesmo tempo informado pelo remetente.

Existem diferentes mecanismos para prover cada tipo de não-repudiação, sejam eles baseado na confiança de uma terceira entidade ou por outros procedimento adotados no processo de geração da assinatura a entrega do documento. Uma boa perspectiva de mecanismo deve envolver pelo as cinco atividades distintas abaixo citadas, que ocorrem na seguinte ordem:

1. Requisição de serviço: acordo entre as partes envolvidas com relação as formas de garantia de não repúdio que se farão necessárias na comunicação e a solicitação destas;

2. Geração de evidência: a parte que é considerada o potencial repudiador deve seguir a regra de geração de evidência. A evidência pode consistir da informação que é parte integrante da comunicação, ou pode incluir informações que são providas separadamente da comunicação primária;

3. Transferência de evidência: a evidência gerada no passo anterior deve ser transferida a(s) parte(s) que possa(m) vir(em) a utilizá-la(s);

4. Verificação de evidência: o serviço requisitante (ou designado) deve verificar se a evidência fornecida é suficiente para prover suporte para não repudiação em eventos no caso de disputas;

5. Retenção de evidência: o serviço requisitante deve manter a evidência para que seja possível a recuperação para uso futuro. O requerente de serviço pode executar a retenção ou arquivamento da evidência, mas a força de evidência de não repúdio em alguns casos serão sustentadas se existir confiança em uma terceira parte que ofereça disponibilidade e credibilidade nas evidências fornecidas.

3.4.3 Originalidade

No documento papel, cópias podem ser constatadas e diferenciadas das suas originais, pois os mesmos apresentam características físicas passíveis de verificação, como a reprodução obtida através de uma fotocopiadora.

Entretanto em documentos eletrônicos, sua reprodução gera uma cópia fiel documento, ou seja, exatamente igual ao seu original. Assim, o conceito de originalidade e cópia deixa de fazer sentido em documentos eletrônicos.

Para alguns documentos isso é extremamente imprescindível, pois sem a possibilidade de verificação da originalidade, não há razão de existir. O dinheiro é um exemplo que torna mais claro essa afirmação; pois em papel ele pode prover de diferentes formas de assegurar a não reprodução, como a utilização de papéis especiais, marcas d'água e fios de proteção. Se essas formas não fossem empregadas, poderia ocorrer um derrame de notas falsas.

Documentos eletrônicos com essa finalidade normalmente estão associados a procedimentos que devem ser executados de forma a garantir a originalidade.

3.4.4 Aspecto Temporal

Documentos papel sofrem ação do tempo, mudam de cor e desgastam, também podem ser datados durante sua confecção e autenticados com reconhecimento de firma em cartório, o qual consta data, dando fé pública a este. O mesmo não ocorre no mundo digital, pois estes documentos não sofrem qualquer alteração aparente em decorrência do tempo de existência, e mesmo existindo a possibilidade de inclusão de data para fazer referência ao tempo, isso pode ser facilmente alterado.

A confiabilidade de documentos eletrônicos está diretamente relacionada ao aspecto temporal.

Na assinatura digital, a ligação entre o documento e o autor, no caso o signatário, ocorre por meio de um certificado que está ligado a duas chaves (pública e privada), o qual pode ser revogado, seja por ocorrência da expiração do prazo de validade ou pela solicitação da revogação por comprometimento da chave.

O aspecto temporal relacionado ao documento eletrônico é fator muito importante para garantir sua integridade, uma vez que data/hora são facilmente alteráveis, e no caso de disputa, se torna imprescindível que isso seja confiável e passível de verificação [DB 91]. Além da integridade, sem a datação, os documentos teriam validade apenas

durante o tempo de vida do certificado digital associado a assinatura.

Um cenário pode ser criado para exemplificar o que a ausência desse fator ocasionaria. Um pedido de compra de um veículo é emitido na forma eletrônica, assinado digitalmente e enviado a uma revendedora. Esta submete o documento ao processo de verificação, e constata que a assinatura é autêntica. Porém no ato da entrega do veículo, o titular do pedido de compra nega a autoria do pedido. O cancelamento desse pedido gera gastos, tais como o transporte do veículo da fábrica a revendedora, criando uma situação de disputa em torno de quem assume estas despesas. Pode ter ocorrido três situações, perante este cenário:

- O solicitante da compra emite a guia para a revendedora, porém depois constata que não quer mais concretizar essa compra, e quer reincidir o contrato de compra e venda sem arcar as custas de rescisão do contrato. Assim ele solicita a revogação do certificado e no ato da entrega do bem, alega que não ter sido o responsável pela emissão deste documento, que o mesmo foi gerado após a revogação do certificado e a data constante foi alterada pela revendedora para validar o pedido;

- A revendedora recebe o pedido e verifica que o documento confere a assinatura, porém constata que o certificado foi revogado por algum motivo. Mas a revendedora tem outro pedido na mesma cidade, e agindo de má fé, altera a data da emissão do documento para algum tempo antes da solicitação de revogação do certificado, desta forma, envia o veículo, porém imputa a responsabilidade do pedido ao titular do pedido de compra, para que desta forma não necessite ter gastos com frete do transporte deste veículo;

- Pode ter sido verificado o comprometimento da chave do titular do pedido de compra e solicitado a revogação do certificado correspondente a esta chave em algum tempo antes da emissão do pedido de compra. O elemento malicioso que comprometeu a chave, solicita a compra do veículo em nome do titular do certificado a qual pertence a chave que ele conseguiu obter, porém gera este documento com data retroativa, assina e encaminha para a revendedora. Como a assinatura confere, esta autoriza a entrega do veículo.

Para cada caso existiu um elemento malicioso: o solicitante da compra, a revendedora e um terceiro elemento, respectivamente. Se este pedido não possuir data e hora confiável, não existe uma forma de detectar quem é o elemento malicioso e, portanto, não é possível resolver esta disputa. Desta forma, justifica-se a grande importância da confiabilidade do tempo em um documento digital.

Não somente nestes casos a data dos documentos é um fator importante, pois nos casos de dúvida ou impugnação dos litigantes, em documentos particulares, a lei 5869, art.370, baseia-se na datação dos itens por ela composta.

No sentido de solucionar este problema, pode adotar-se o processo de protocolação dos documentos eletrônicos. A protocolação digital visa vincular uma data e hora confiável a um documento específico, que atenda a necessidade da preservação do valor jurídico por longo período de tempo.

Existem duas formas de realizar a protocolação digital: a que exige uma terceira entidade confiável (Trusted Third Party - **TTS**) e as que se baseiam na confiança distribuída. A primeira, consiste na imparcialidade da **TTS**, a entidade responsável pela protocolação do documento eletrônico; enquanto técnicas baseadas na confiança distribuída, o documento é submetido a vária pessoas, que datam e assinam o mesmo, partindo da conjectura de que não é possível corromper todos os elemento envolvidos no processo para geração de data falsa.

A segunda técnica é muito frágil, pois pode ser facilmente forjado um grupo que acordem em falsificar essa data, como exemplo, diversos pessoas com interesse em comum, datam e assinam um documento com o horário que tenham interesse, se a o verificador não conhecer a ligação entre desse elementos e confiar nesta data/hora, poderá estar aceitando um documento que não apresente um dado verídico.

Em contrapartida, a protocolação através de uma **TTS**, Autoridade de Datação (**AD**), ou Protocoladora de Datação Documento Eletrônicos (**PDDE**), ela deve atender diversos requisitos que garantam que não exista formas que habilitem a AD a subverter a datação do documento, mesmo que isso seja intencional, atribuindo dessa forma data/hora válida e confiável para documentos eletrônicos.

Se esta cumprir satisfatoriamente e forma confiável estes requisitos, o

problema do documento eletrônico em relação ao aspecto temporal do momento da assinatura é solucionado.

3.5 Conclusão

A definição de documentos eletrônicos para que possuam valor jurídico e atendam no mínimo os mesmos requisitos garantidos pelos documentos papel não é uma tarefa fácil e ainda encontra-se em estudo e desenvolvimento. Como visto são muitos elementos e atributos que devem ser supridos e nem todos possuem propostas ou técnicas implementas.

Capítulo 4

Impactos Jurídicos e Tecnológicos da Regulamentação da Assinatura Digital

4.1 Introdução

Com o advento da validade jurídica dos documentos eletrônicos no Brasil, diferentes segmentos serão atingidos pelo impacto dessa inovação. Os cartórios serão as instituições que deverão sofrer diversas adaptações para garantir a fé pública em documento na forma eletrônica. Novos métodos deverão ser criados e adotados de forma a garantir no mínimo a mesma confiabilidade provida ao documentos na forma papel.

Para isso é de fundamental importância observar aspectos das assinaturas eletrônicas em relação a sua validade jurídica. Por exemplo, por quanto tempo a tecnologia utilizada para gerar a assinatura eletrônica será considerada válida? Como garantir que assinaturas em documentos eletrônicos não sejam forjadas no caso do emissor não poder se manifestar? Os softwares para verificação de assinaturas digitais são confiáveis? Como solucionar impasses em relação a falsificação de assinaturas?

As questões supra citadas serão abordadas no decorrer do capítulo, onde a primeira seção descreve de forma sucinta o cartório atual e as adaptações que deverão sofrer. Na seção 4.6 são discutidas o tempo de validade de vida útil de uma assinatura digital e formas para garantir sua longevidade. Na seção 4.4 são mencionados a dependência

da confiabilidade do software de verificação de assinatura, os métodos existentes e os elementos envolvidos em uma disputa judicial relacionada a assinaturas.

4.2 Estrutura Cartorária do Brasil

Os cartórios são instituições privadas, às quais o Estado concede fé pública, através de concurso público de provas e títulos, conforme mandamento constitucional (art.236 parágrafo 3), estando sujeitos a responsabilização civil e criminal.

A aprovação da medida provisória 2.200-1 em 27/07/2001, a qual regulamenta a infra estrutura de chave pública, visando a garantia da autenticidade, integridade e validade jurídica de documentos na forma eletrônica, assim como as aplicações de suportes, aplicações habilitadas que utilizem certificados digitais e a realização de transações eletrônicas seguras [dA 01].

Ao longo da história cartorária, os documentos tratados sempre apresentaram-se na forma papel. Dessa forma, esse sempre foi o meio físico utilizado no ateste da validade de fé pública, seja para aposição de carimbos e assinaturas, ou emissão de registros, certidões ou cópias em livros. Então pode pensar-se que está próximo do fim as instituições cartorárias? Pelos diversos fatores já apresentados em relação as facilidades de documentos na forma papel, isso garantirá a manutenção dessa estrutura por longo período, mas sem dúvida deverão sofrer adaptações nos serviços prestados ou novas instituições que deverão surgir no intuito de prover a fé pública em documentos eletrônicos.

Entretanto surge também o questionamento em relação a atuação de empresas privadas no ramo de negócios jurídicos, tendo em vista a possibilidade de falência e as especificidades da Internet em que as empresas têm sede virtual. "Talvez uma solução seja uma regulamentação bem detalhada e uma fiscalização operante, até porque a atribuição de fé pública é ato de extrema importância, exigindo cautela e bastante critério"[dA 01].

O setor cartorário ainda caminha em passos lentos no sentido da adoção de documentos eletrônicos,porém projetos desenvolvidos por tabeliães e associações de

cartórios já prometem mudar essa imagem, buscando a modernização que vão da ligação de cartórios em rede, emissão remota de certidões até a certificação digital. Devendo prover serviços equivalentes ao registro de assinatura eletrônica, reconhecimento de firma digital e autenticação eletrônica[BAT 01].

A nova estrutura cartorária deverá atender diversas necessidades originadas pelo documento eletrônico. Os papéis já desempenhados, deverão sofrer adaptações, pois passarão a ter novas atribuições. Em algumas situações o reconhecimento de firma não será suficiente para garantir a validade jurídica do documento eletrônico se realizada na forma tradicional.

Com documentos na forma papel, a assinatura uma vez aposta sobre o documento, pode ser passível de prova e garantia de autenticidade a qualquer tempo. Já em documentos eletrônicos nem sempre a assinatura é assegurada, mesmo que ela possua o selo de datação. Um exemplo é o caso do testamento que passa a ter valor após o falecimento do signatário. Sob a forma papel, a autenticidade da vontade expressa no documento poderá ser verificada através da assinatura manuscrita com o reconhecimento de firma emitido por um cartório. Já na forma eletrônico o reconhecimento não garante que o documento não é um objeto de fraude. Numa situação hipotética, Alice tem sua chave privada comprometida por um elemento malicioso (Maria). Esta gera um testamento falso em nome de Alice e assina com a chave privada de Alice que conseguiu obter. Submete o documento a uma AD de documentos eletrônicos para atribuir data/hora, e depois não utiliza a chave em nenhum momento. Assim Alice não descobrirá que sua chave foi comprometida, e caso Alice morra e não deixe nenhum testamento, Maria possui um testamento com uma assinatura autêntica e com data anterior ao falecimento de Alice.

Este é um exemplo onde o reconhecimento de firma da forma tradicional não é suficiente. Documentos que tratam de valores expressivos, ou de dados com alto grau de sensibilidade, para que adquiriram valor legal, devem ser submetidos a uma nova política de autenticação. Neste caso, quem apõe a firma deve estar fisicamente presente diante do notário, o qual é o responsável pela verificação do status do certificado, identificação do signatário e a integridade do documento antes de dar o ateste na assinatura.

4.3 Autenticação

A autenticação de um documento é o ato do reconhecimento de um escrito como verdadeiro e o grau de segurança desse fator deve estar ligada a importância da informação contida no documento.

Assim como nos documento papel, onde diferentes situações exigem segurança adicional, nos documentos eletrônicos esses graus de segurança também podem ser proporcionados, através diversos de fatores.

No documento eletrônico a assinatura digital é um código binário que é determinado com base no documento, e que associa este a uma determinada pessoa ou conjuntos de pessoas. Essa associação é conhecida como autenticação dentro da classificação dos seus níveis de confiabilidade podem ser classificadas como:

- fator 1: algo que se sabe;
- fator 2: algo que se tem;
- fator 3: algo que se é;
- fator 4: localização espacial e temporal;
- fator 5: testemunhas.

O fator um é o que apresenta menor nível associação, pois baseia-se em algo que se sabe, como por exemplo uma senha. Isso pode ser facilmente obtido ou compartilhado com outra pessoa, assim mais de uma pessoa estará hábil a autenticar-se por outra.

O fator dois a identificação ocorre por meio de algo físico, como um crachá ou uma autorização de acesso, mas normalmente este nível é empregado juntamente com nível um. Exemplos dessa junção são cartões magnéticos e smart cards. Apesar de garantir um maior confiabilidade, ainda é possível existir personificação.

A autenticação baseada em algo que se é, pode se considerada a ideal, pois a identificação exige um alto grau de dependência com a pessoa que esteja

submetendo-se a identificação. Esse nível utiliza dados biométricos, ou seja, características físicas, como a íris dos olhos, impressão digital, geometria do rosto, etc. A biometria é eficiente, pois o ser humano possui características corporais únicas e que são, de certa forma, estáveis e intransferíveis,

Nos dois primeiros fatores a identificação pode ser esquecida, roubada, perdida e até mesmo revelada. Já a autenticação por dados biométricos, como impressões digitais podem ser convertidos em códigos de barras, os quais estão livres dessas desvantagens.

Um nível maior de segurança na autenticação pode ser alcançado através do incremento dos seguintes fatores: testemunhas e/ou localização, ou seja, fatores 4 e 5 respectivamente. Estes fatores podem ser associados aos fatores anteriores (1,2,3) a fim de tornar a tarefa de personificação quase impossível.

A autenticação associada a localização temporal e espacial, somente considera válida a assinatura se for realizada nos locais e horários previamente definidos. Por exemplo, a assinatura de um acionista de uma empresa, para autorização de saque acima de determinado valor somente pode ser feita na sala de reuniões da empresa no horário de expediente do acionista. Assim, caso ele queira dar um golpe na empresa, ou é sequestrado e seja obrigado a realizar a assinatura em qualquer outro lugar ou horário, essa ação poderá ser realizada, porém não produzirá assinaturas válidas.

O fator de autenticação por testemunhas, implica adicionar a ligação da assinatura a uma entidade ou pessoa. Uma assinatura é considerada válida somente se contiver junto ao documento o ateste de testemunha de um segundo elemento através da assinatura deste.

Um exemplo a ser considerado é a ligação da assinatura a um órgão confiável, como um cartório. Assim para a validar uma assinatura, o signatário deve apresentar-se no órgão e perante um cartorário realizar a operação de assinatura, e este, ao presenciar o ato assinar atestando.

Este processo é semelhante ao já existente para documento papel onde para determinados tipos de documentos, como a transferência de um veículo, esse procedimento já é adotado.

4.4 Software de verificação de assinatura

Para prover o reconhecimento de firma digital, a instituição responsável por prover a validade jurídica do documento deverá realizar a verificação da assinatura digital. Até o momento, este procedimento era feito somente em documentos na forma papel. Quando este documento era submetido ao processo de verificação, a assinatura manuscrita aposta sobre o papel era comparada com o cartão de assinatura previamente preenchido e mantido na instituição, do pressuposto signatário. As assinaturas então eram comparadas na instituição cartorária e se reconhecida, o documento recebia assinatura do tabelião e o carimbo com data.

Em documentos eletrônicos essa tarefa é totalmente diferente, a visualização da assinatura não pode ser feita sem a utilização de um software que dê suporte, e a sinalização de reconhecimento de firma também exige novos requisitos. Então o software de visualização e conferência da assinatura digital para estas instituições deve apresentar não somente grande precisão, mas acima de tudo confiabilidade, uma vez que através deles são conferidas fé pública aos documentos.

Emerge a necessidade da criação de dispositivos legais padronizados que atendam estes requisitos e que não restrinja o uso de nenhuma tecnologia, afim de acompanhar o desenvolvimento tecnológico e escapar de tendências monopolistas de determinadas empresas.

4.5 Validação Jurídica da Cópia Impressa

A expansão da utilização de documentos eletrônicos trouxe a necessidade de meios que garantissem a autenticidade e integridade da informação, para que documentos eletrônicos pudessem ter a mesma aplicabilidade do documentos papel. Agora, deve-se buscar também mecanismos que garantam a validade jurídica de um documento eletrônico sob a forma impressa.

A assinatura digital é facilmente verificada em documentos na forma digital, mas se o documento for simplesmente impresso, essa verificação deixa de ser

possível. O processo que garanta essa transição de formatos sem perda de valor legal do documento, pode ser provida através de instituições cartorárias.

A estrutura dos cartórios, uma entidade considerada confiável, pode ser utilizada para promover a validação da assinatura em documentos eletrônicos. O reconhecimento de firma de um documento eletrônico exigiria que o mesmo fosse submetido na forma de um arquivo, podendo ser em um disquete ou por e-mail. O cartório verificaria a assinatura digital da forma usual, caso fosse verdadeira, imprimiria a informação, a identificação do signatário e protocolaria. Assim o documento gerado através de transações eletrônicas pode ser materializado e permanecer com a assinatura válida.

Novamente deve-se considerar o aspecto da datação nos documentos, pois os mesmos devem apresentar esse atributo para que os cartórios possam verificar se a validade do certificado digital no momento da assinatura. Diferentemente da assinatura escrita (em documento papel), desde que autêntica, se manterá válida; enquanto o certificado digital, associado a chave da assinatura pode ser revogado por diversos fatores como (roubo da chave privada, vencimento do certificado). Assim documentos eletrônicos assinados após o horário de um pedido de revogação do certificados não devem ter seu reconhecimento efetuado.

4.6 Período de validade jurídica do documento assinado

Uma vez aposta a assinatura em documentos papel, elas podem ser conferidas e ter validade por tempo indefinido. Este reconhecimento pode ser dado através de exames grafotécnicos, pela fé pública concedida por um Tabelião, ou outros procedimentos reconhecidos legalmente como os selos das Autoridades públicas.

No mundo digital, ainda não existem formas que atendam a necessidade da garantia da prova de existência de acordo, sem vínculo da validade jurídica a um prazo de validade, pois a vida útil de um documento assinado digitalmente está ligada a segurança do algoritmo de chave pública e a função de resumo utilizada para gerar a assinatura.

A submissão do documento eletrônico assinado a uma protocoladora

digital, conforme citado no item anterior, garante sua confiabilidade até que a segurança deste mecanismo não possa ser comprometida pela tecnologia computacional existente. Assim faz-se necessário o estudo de técnicas operacionais viáveis, para que após o período de garantia de confiabilidade do mecanismo de assinatura e/ou datação utilizado, o documento mantenha a propriedade da integridade de informação, autoria e tempo.

4.7 Leis existentes para garantia da aceitação do documento eletrônico

Em 1998, os Estados Unidos aprovou o Government Paperwork Elimination Act (**GPEA**)[1], uma lei que tem como objetivo promover o uso da comunicação e comércio na forma eletrônica em transações entre o público e o governo federal.

O **GPEA** requer que agências Federais produzam versões eletrônicas de seus documentos e formas on-line disponíveis que permitam que indivíduos e empresas usem assinaturas eletrônicas para arquivar os documentos na forma eletrônica[HOU 01] .

Todas as organizações que lidam com o governo federal serão afetadas pelo **GPEA**. As agência do governo e organizações que são provedoras de serviço do governo federal, vão sofrer um impacto significativo em seu processo empresarial e os tribunais passam a não poder rejeitar um documento digital só porque não está na forma papel[PUR 01].

No mesmo sentido a Europa estabelece uma plataforma legal para garantir o reconhecimento de assinaturas digitais, especificando que estes documentos eletrônicos não possam ser discriminados legalmente em decorrência da sua forma.

No Brasil,a proposta de política de governo eletrônico, elaborada pelo *Grupo de Trabalho Novas Formas Eletrônicas de Interação para o Poder Executivo Federal* cita a *"regulamentação do uso, validade e condições gerais para a efetivação do documento eletrônico como um documento legal de uso pleno, até dezembro de 2001, visando a eliminação do uso de papel na documentação governamental, até dezembro de*

[1]Lei aprovada em 23/10/1998 disponível em http://www.cdt.org/legislation/105th/digsig/govnopaper.html

2006."

O projeto de lei n. 1.589, de 1999, da Câmara dos Deputados, elaborado a partir de anteprojeto da Comissão de Informática Jurídica da OAB/SP, dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital. Adota o sistema de criptografia assimétrico como base para a assinatura digital e reserva papel preponderante para os notários. Com fundamento no art. 236 da Constituição e na Lei n. 8.935, de 1994, estabelece que a certificação da chave pública por tabelião faz presumir a sua autenticidade, enquanto aquela feita por particular não gera o mesmo efeito.

4.8 Conclusão

O fenômeno Internet vem sendo objeto de normatização, em seus diferentes aspectos, em vários países do mundo e em organismos internacionais. Esse é um importante passo dado para o adoção definitiva do documento eletrônico, e o governo brasileiro também deve ater-se a importância da legislação e medidas que outros países vêm adotando nesse sentido de promover a utilização e aceitação de documentos eletrônicos em substituição a documentos papéis.

Porém não se pode deixar de observar que a validade jurídica dos documentos eletrônicos depende de alguns fatores não existentes nos documentos papel, muitos deles críticos na validação jurídica, tornando necessária a revisão dos métodos tradicionais no tratamento de documentos, como por exemplo a atribuição de fé pública.

Capítulo 5

Codificação de Documentos Eletrônicos

5.1 Introdução

Neste capítulo são descritos os paradigmas de gerenciamento da informação (organização, recuperação e uso), que surgiu com o padrão das linguagens denominadas de marcação (ou "markup languages").

Estas linguagens identificam de forma descritiva, cada "entidade informacional"digna de significado presente nos documentos, como por exemplo, parágrafos, títulos, tabelas ou gráficos. A partir destas descrições, os programas de computador podem melhor compreender e, em conseqüência melhor tratar ou processar a informação contida em documentos eletrônicos.

A informação e o computador são parceiros antigos, mas a intensificação e democratização do seu uso, aliada à abstração sempre crescente do nível de manipulação/interação e troca de informações criou terreno propício para a origem das chamadas linguagens de marcação. Padrões públicos e abertos que foram criados, no início, para tentar maiores avanços no tratamento da informação; para minimizar o problema de transferência de um formato de representação para outro, enfim, para liberar a informação das tecnologias de informação proprietárias.

Na seção 5.2 é feita uma introdução sobre linguagens de marcação, sua origem e finalidade. A seção 5.4 apresenta o padrão de codificação **ASN.1** definido pela

ISO, e a seção seguinte, descreve os padrões **XML** para assinaturas digitais.

5.2 Linguagens de Marcação

O mundo digital no qual vivemos está repleto de diferentes linguagens de marcação, podendo ser encontradas linguagens de marcações patenteadas usadas em pacotes de processadores de texto (MS Word ou Corel's WordPerfect), e de editoração eletrônica (Ventura, PageMaker ou Quark).

Existem também linguagens de marcação abertas e sem patentes como TeX, Troff e a mais conhecida, a HTML (HyperText Markup Language - linguagem de marcação de hipertexto).

O **SGML** - Standard Generalized Markup Language é um padrão internacional para descrever documentos eletrônicos. É uma meta linguagem utilizada para escrever outras linguagens. Ele ajuda a descrever documentos de texto de uma maneira lógica e estrutural. **SGML** é usada primariamente para a criação, armazenagem e distribuição de documentos e como uma fonte para conversão para outros documentos.

A linguagem foi reconhecida como um padrão **ISO** (8879) em 1986. **SGML** não é um conjunto pré-determinado de marcas e sim uma linguagem para se definir quaisquer conjuntos de marcas e auto-descritiva. Cada documento **SGML** carrega consigo sua própria especificação formal, o **DT** "Data Type Document".

Porém a especificação da **SGML** é extensa, contendo 300 páginas, enquanto que o **XML**, 33, a qual apresenta uma simplificação do **SGML** contendo idéias concisas.

5.3 XML

XML (Extensible Markup Language) é uma linguagem que permite que qualquer tipo de informação seja distribuída através da Web. As páginas ou formulários baseados em **XML** têm vida própria capaz de processar seus dados, não necessitando de processamento no servidor.

O **XML** fornece uma representação estruturada de dados que pode implementada a partir de um grande número de aplicações, sendo de fácil extensão. **XML** é um subconjunto da **SGML**, apropriado para distribuição pela WWW; a partir da definição conferida pela W3C, que tinha como objetivo propor uma simplificação do **SGML**, e que garantisse que os dados estruturados fossem uniformes e independentes de aplicações ou distribuidores.

XML é atualmente um padrão que permite o desenvolvimento de aplicações baseadas na Web que necessitem de formulários eletrônicos integrados com diversos sistemas, estes formulários podem conter dados, imagens, assinaturas eletrônicas, lógica, e entre outros atributos.

O formato **XML** pode ser definido para assinaturas eletrônicas avançadas para que permaneça válida por longo período de tempo. Isto inclui evidências de validade até mesmo se o signatário ou as partes tentar negar (repudiar) a validade da assinatura.

O **XAdES** (XML Advanced Electronic Signatures) é o formato básico para assinatura digitais, proposto pelo **ETSI** (European Telecommunications Standards Institute), conforme ilustra figura 5.1,

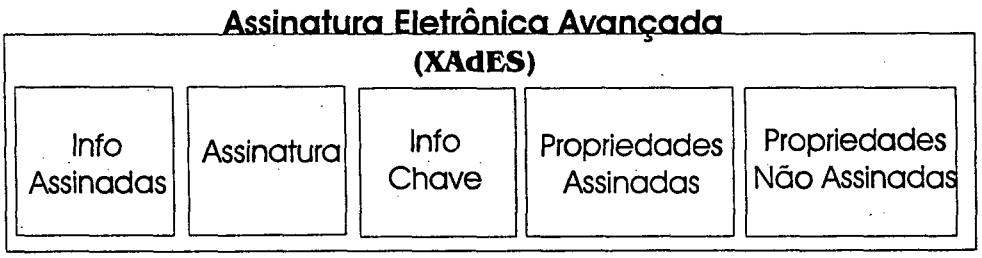

Figura 5.1: Padrão XML- XAdES: Formato padrão proposto pelo ETSI de assinaturas digitais avançadas.

Existem diferentes formas definidas de assinaturas eletrônicas, cada uma satisfazendo certas exigências [ele 01]:

- Advanced Electronic Signature (XAdES);
- XAdES com selo de tempo (XAdES-T);

- XAdES com Validação Completa dos dados (XAdES-C);
- XAdES-X e XAdES-X-L, formas extendidas do XAdES;
- XAdES-A possibilita uma seqüência de selos de tempo;

O formato dos três primeiros formatos são definidos com a adição de propriedade assinadas (SigningTime, SigningCertificate, SignaturePolicyIdentifier, SignatureProductionPlace, SignerRole, ContentTimeStamp, DataObjectFormat e CommitmentTypeIndication) e propriedades não assinadas (CounterSignature).

O **XML-ES** com selo de tempo (**XAdES -T**) adiciona um selo de tempo ao **XAdES** como iniciativa para prover termo de validade por longo período, sendo esta uma forma de registro do tempo da criação para prover proteção contra repúdio.

O **XML-ES** com dados de validação completos (**XAdES-C**), adiciona ao **XAdES-T** as referências para o conjunto de dados que suportam a validade da assinatura eletrônica (ou seja, as referências restantes para o caminho de certificação e sua informação de estado de revogação associada).

A figura 5.2, mostra os formatos padrões XML-ES, XAdES-C e XAdES-T.

Figura 5.2: Formatos XAdES-C e XAdES-T: extensão do formato XAdES, incluindo atributos de selo de tempo (XAdES-T) e dados para verificação da assinatura (XAdES-C).

Outros dois formatos adicionais são definidos pelo **ETSI**, o **XAdES-X** e **XAdES-A**. O **XAdES-X** tem como objetivo prover garantia sobre do caminho de certificação e revogação do documento, através da geração de um selo de tempo sobre o formato **XAdEs-C**.

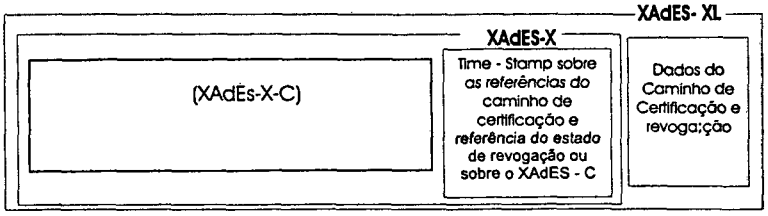

Figura 5.3: Formatos XAdES-X-L: Ilustração dos formatos XAdES-X e XAdES-X-L

O formato **XADeS-A**, adiciona um novo selo de tempo antes que o algoritmo, ou chaves utilizadas se tornem fracas e vulneráveis, com objetivo de garantir a renovação da tecnologia utilizada antes do seu comprometimento pelo poder computacional existente para quebra do algoritmo criptográfico utilizada na assinatura e/ou datação, permitindo o arquivamento do documento.

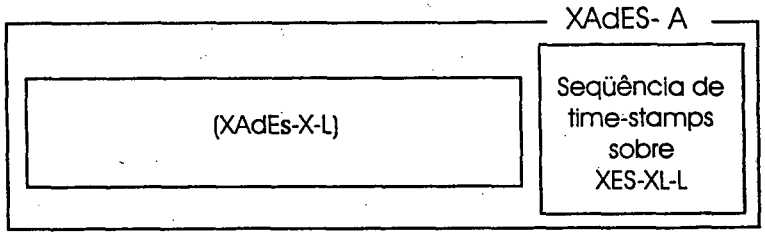

Figura 5.4: Padrão XAdES-A: Formato que suporta a renovação da tecnologia utilizada para assinar o documento.

5.4 ASN.1

Aplicações remotas necessitam de padrões para comunicação(semântica), pois durante a transferência dos dados não são envolvidas detalhes da representação das informações (sintaxe de transferência) ou codificação durante a comunicação.

O nível de apresentação que definem a sintaxe a comunicação através do uso de regras de codificação e provê um serviço comum a todas aplicações, negociando a sintaxe de transferência dos dados. Assim, o nível de apresentação pode receber os dados do nível de aplicação estruturados de acordo com uma sintaxe de apresentação,

reestruturá-los de acordo com a sintaxe de transferência e o nível de apresentação receptor, pode ainda, tornar a promover uma restruturação dos dados para apresentá-los ao seu nível de aplicação de uma forma compreensível para este.

Em situações onde a sintaxe de apresentação dos dados é diferente entre as entidades que interagem, é necessário que haja formas de negociação de transferência a ser utilizada, para isso é preciso poder no mínimo, referí-la por um identificador ou ainda, definí-la e associar-lhe um identificador ou nome. Esta associação entre um conjunto de valores de dados e sua representação constitui o que é denominado um contexto de apresentação definido.

A **ISO** definiu uma notação (**ISO** 8824 e **ISO** 8825, derivada da recomendação CCITT X.409) que permite definir tipos de dados simples e complexos, e os valores que podem ser atribuídos. Esta notação é denominada Notação para Sintaxe Abstrata Um (**ASN.1** Abstract Sintax Notation One). Esta notação que não indica o valor dos dados, apenas sua forma. Além disso existem algoritmos, denominados Regras Básicas de Codificação (Basic Encoding Rules) que determinam o valor dos octetos representando tais valores e que serão passados para o nível de sessão (isto e denominado a sintaxe de transferência de dados).

ASN.1 ou Abstract Syntax Notation One é uma notação que permite definir tipos de dados simples e complexos e especificar valores que estes tipos podem assumir. As regras de codificação constituem outro padrão que aplicadas ao valor de um certo tipo definido pela **ASN.1** resultam na especificação completa dos valores daquele tipo durante a transferência. As regras de codificação sempre forçam a transmissão do rótulo de um tipo, implícita ou explicitamente, juntamente com a representação do seu valor.

Os valores que são transmitidos podem ser de diversos tipos. Existem os tipos simples e outros, mais complexos, que são formados de vários tipos simples combinados. Cada tipo recebe uma denominação que o distingue, de forma inequívoca de todos os demais tipos. Algumas das maneiras de definir novos tipos são: uma seqüência (ordenada) de tipos existentes, uma seqüência não ordenada de tipos existentes e uma seleção de um dentre um conjunto de tipos.

Estes são denominados tipos estruturados. Cada tipo recebe um rótulo ("tag"). Um mesmo rótulo pode ser atribuído a mais de um tipo cuja particular identificação será decidida pelo contexto em que o rótulo for usado.

Existem quatro classes de rótulos:

- UNIVERSAL: pode ser atribuído a um tipo simples ou a um mecanismo de construção.
- APLICAÇÃO: rótulos atribuídos a tipos por padrões específicos. Num particular padrão os rótulos da classe de APLICAÇÃO somente podem ser atribuídos a um único valor.
- PRIVADA: rótulos usados numa empresa especifica.
- ESPECIFICADO-POR-CONTEXTO: interpretado de acordo com o contexto em que é usado.

5.5 Conclusão

A existência de formatos padrões para documentos eletrônicos, os quais incluem atributos de validação da assinatura digital é muito importante devido a facilidade de interoperabilidade, como também na recuperação quando armazenado por longo período de tempo.

A proposta apresentada pela ETSI, o XAdES-A, prevê a possibilidade da renovação da tecnologia antes do seu comprometimento, porém não mostra os procedimentos necessários que garantam estes processos.

Capítulo 6

IARSDE - Infra Estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos

6.1 Introdução

Os problemas relacionados ao tempo de validade do documento eletrônico não se concentram apenas na manutenção da assinatura digital, pois sua existência também está ligada ao meio onde foi criado (software) e armazenado (mídia). Assim novos problemas estão associados à recuperação de documentos eletrônicos armazenados por longo período de tempo.

Atualmente ao pensarmos em softwares para criação de documentos eletrônicos torna-se importante relacioná-los ao mantenedor no meio digital, por ser parte integrante da possibilidade de preservação. Ainda deve-se considerar a importância da existência de novas alternativas de armazenamento para que seja possível conviver com o avanço da tecnologia do meio escolhido e suas fragilidades, de forma a garantir a permanência dos registros digitais.

Este capítulo apresenta uma proposta de uma infra estrutura com objetivo de armazenamento e recuperação de documentos eletrônicos por longo período de

tempo a qual assegura a manutenção dos seus atributos legais.

6.2 Visão Geral da IARSDE

A **IARSDE** (Infra Estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos), proporciona o armazenamento e recuperação de documentos eletrônicos provendo o controle da expiração da validade da tecnologia utilizada para assinatura e datação, 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.

Para que isso seja possível a IARSDE realiza a integração de três autoridades: Autoridade de Datação (**AD**), que funciona de acordo com os esquemas já existentes, porém com serviços adicionais; Autoridade de Gerenciamento de Depósitos de Documentos Eletrônicos (**AGDDE**), e Autoridade de Garantia de Tecnologia (**AGT**) são definidas juntamente com a proposta da IARSDE.

A **AGDDE** tem como funcionalidade a distribuição e recuperação da informação na rede, garantindo a integridade do documento mesmo nos caso de tentativas maliciosas de subversão da informação mantida nos servidores. Cabe também a função de gerenciamento e agrupamento dos documentos de acordo com a ordem cronológica da validade da tecnologia para o controle da expiração desta, ou seja, a reassinatura.

A **AGDDE** também tem como função garantir de forma segura o documento de acordo com o modo de armazenamento escolhido pelo submissor do documento.

A **AD** possui a função de protocolar documentos atribuindo data e hora, e também informar a previsão da garantia máxima da tecnologia utilizada na assinatura do documento e do selo de tempo emitido por ela. Esse atributo é obtido através de consultas as listas de previsão de comprometimento da tecnologia, mantidas pela **AGT**.

A **AGT** é a autoridade que tem como função a manutenção das datas relacionadas às expectativas do comprometimento da tecnologia. Para isto, são realizados inúmeros cálculos sobre diferentes tecnologias existentes para definir o grau de dificuldade de quebra do algoritmo em conjunto com tamanho da chave e estimar um tempo de

confiabilidade.

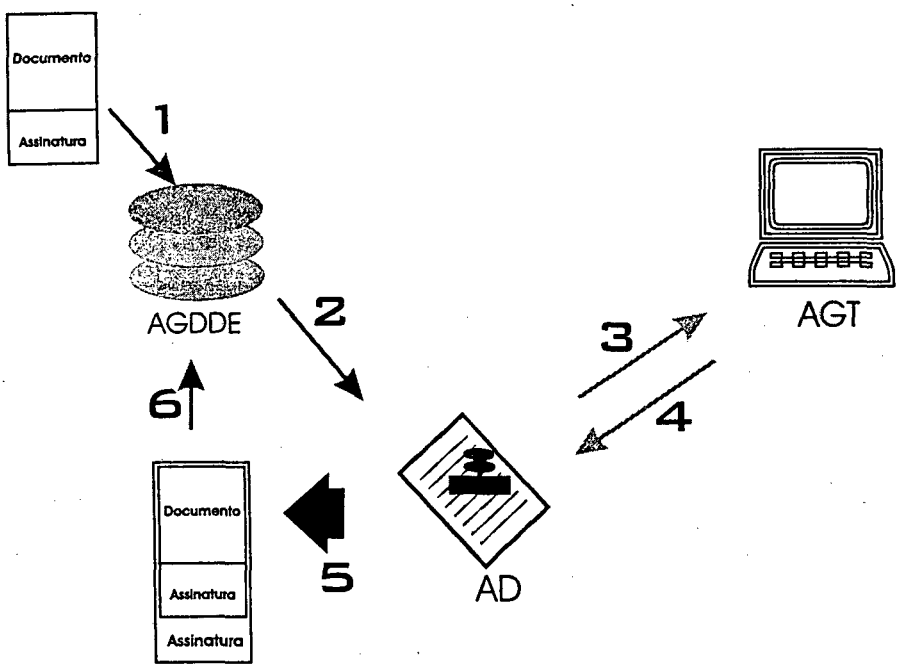

Figura 6.1: Visão Geral do funcionamento da IARSDE: 1. A AGDDE recebe os documentos, organiza e armazena-os. 2. No prazo de validade da tecnologia, a AGDDE envia-os para AD para renovação. 3. A AD consulta as datas da tecnologia utilizada na reassinatura. 4. A AGT responde a solicitação da AD. 5. Os documentos passam a ter uma nova assinatura a partir do encapsulamento da assinatura anterior. 6. A AD reenvia os documentos a AGDDE, que os armazena novamente até a próximo vencimento da validade da tecnologia.

A figura 6.1 apresenta as principais etapas da manutenção e atualização das propriedades do documento eletrônico. Estas etapas e autoridades envolvidas são explicadas com maiores detalhes nas próximas seções.

6.3 Software Padrão de Assinatura Digital - SPAD

Como exposto nos capítulos anteriores, diversos fatores implicam na necessidade da confiabilidade no software que realiza e verifica assinaturas digitais. Porém surge a questão: como saber em qual software confiar?

O governo americano possui um órgão o NIST (National Institute of

Standards and Technology), o qual é responsável por testar e padronizar os softwares oficiais utilizados naquele país. Esta é uma entidade idônea e que possui credibilidade perante os cidadãos americanos. Dessa maneira os softwares padronizados como o DES (Data Encryption Standard), aprovado para uso governamental em 1977 pela National Bureau of Standards.

O Brasil necessita da elaboração de um software padrão para realizar assinatura digital e um software padrão para verificação da assinatura em documentos eletrônicos.

Nesta seção apresentamos uma proposta de software de assinatura para documentos eletrônicos. O software tem como objetivo produzir um documento eletrônico com assinatura digital em um formato padrão que possibilite o processo de reassinatura [1].

As etapas realizadas pelo SPAD para assinatura digital garantem a determinação de um período de tempo da efetivação da assinatura.

Nos processos de geração de uma assinatura digital convencional, o resumo do documento é calculado e depois cifrado utilizando a chave privada associada ao certificado e depois submetido à AD. Isto não possibilita verificar quando a assinatura foi realizada, mas apenas indica o momento em que o documento foi submetido à AD.

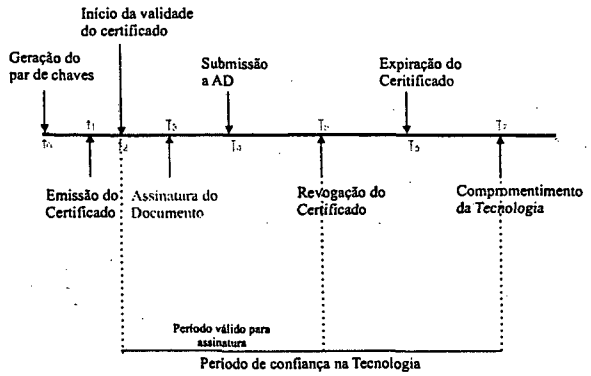

Figura 6.2: Linha temporal da assinatura convencional: tempos de realização das atividades de uma assinatura convencional.

O momento da submissão do resumo do documento assinado à uma AD,

[1] O conceito de reassinatura é apresentado nas próximas seções.

conforme o processo descrito anteriormente, é incorporado os atributos de data e hora. Essas informações garantem que a assinatura ocorreu antes desse tempo, mas não quando foi realizada a assinatura. Conforme é ilustrado na figura 6.2, não podemos verificar que o documento foi assinado em t_3 e submetido à AD em t_4. Só é possível verificar que a assinatura foi realizada antes de t_4. Porém não é possível determinar se ocorreu depois de t_3, podendo até mesmo ter ocorrido entre t_1 e t_2.

A solução para este problema é realizar a datação do resumo antes da assinatura e em seguida, gerar um novo resumo do documento concatenado com o recibo da datação enviada pela AD. Este resumo é submetido a AD em t_3 (ver figura 6.3). No tempo t_4 a AD entrega o recibo de datação do resumo gerado pelo documento original. Em t_5 o documento é assinado. Em t_6 o resumo do documento juntamente com o recibo gerado em t_4 é submetido a AD. Dessa forma é possível determinar um intervalo de tempo em que a assinatura ocorreu.

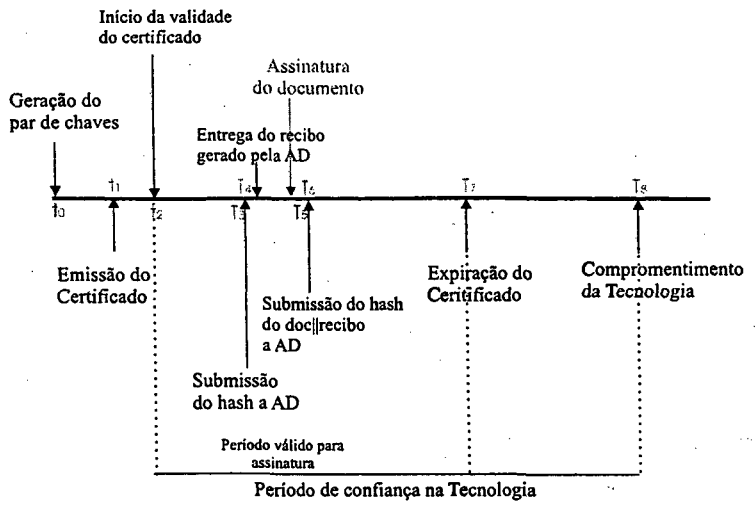

Figura 6.3: Linha temporal da assinatura realizada pelo SPAD: atividades e tempo de realização das atividades pelo SPAD para garantir a assinatura digital com atributos de conferência de intervalo de tempo de realização.

O SPAD constiui-se de uma proposta de um software padrão de assinaturas digitais, o qual tem como funcionalidade a geração da assinatura digital. Este esquema apresenta um padrão de documentos eletrônicos assinados digitalmente, que

visa solucionar o problema do intervalo de tempo da assinatura e reunir dados suficientes para que os documentos possuam os atributos necessários para permitir o processo de renovação de tecnologia, além de estruturar estes dados.

O processo de geração da assinatura e organização do documento é composto no SPAD por três etapas:

- etapa 1: assinatura do documento e determinação do início do intervalo de tempo desta operação;
- etapa 2: submissão do documento a AD para determinar o intervalo de tempo do processo de assinatura iniciado na etapa anterior;
- etapa 3: anexo das informações úteis para armazenamento do documento por longo período de tempo;

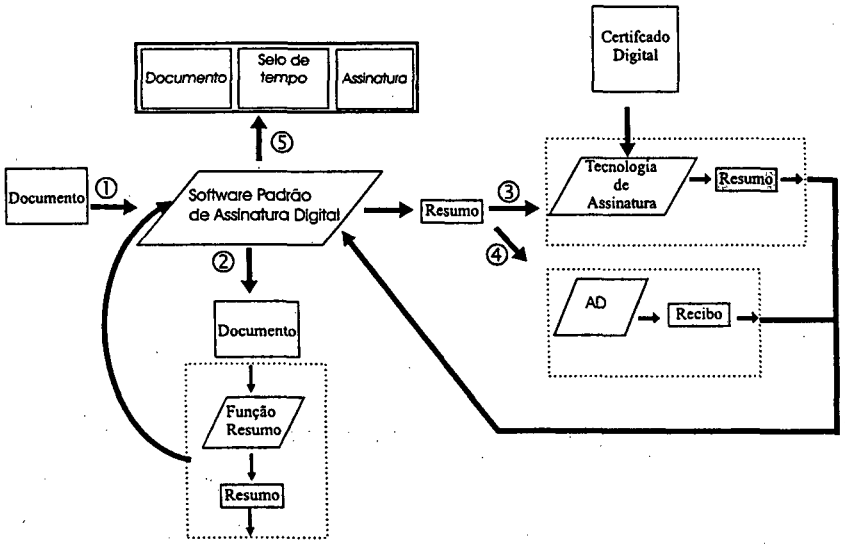

Figura 6.4: Software Padrão de Assinatura Digital - etapa 1: Atividades da primeira etapa da geração da assinatura digital pelo SPAD.

Os processos da **etapa 1**, ilustrada na figura 6.4 consiste na entrega do documento ao SPAD. O documento é submetido a uma função resumo pré-definida que gera o resumo do documento. Sobre este resumo é realizada a assinatura do documento,

cifrando-o com uma tecnologia definida, e a chave privada do signatário. Paralelamente, este mesmo resumo é enviado também a AD para que este receba o atributo de início da geração da assinatura.

Todos estes dados são organizados pelo SPAD, e ao fim da **etapa 1**, o documento estará no formato ilustrado pela figura 6.5.

Figura 6.5: Documento Eletrônico com Assinatura Digital ao fim da etapa 1 do SPAD.

A **etapa 2** procede o cálculo do resumo do documento resultante da etapa 1 (figura 6.7), ou seja, o documento, a assinatura e o selo tempo de tempo do início do processo de assinatura. Este resumo é enviado a AD, juntamente com informações do certificado. A AD protocola o resumo, atribuindo data e hora; que serão os parâmetros de indicação do término do intervalo da realização da assinatura, expresso na figura 6.6.

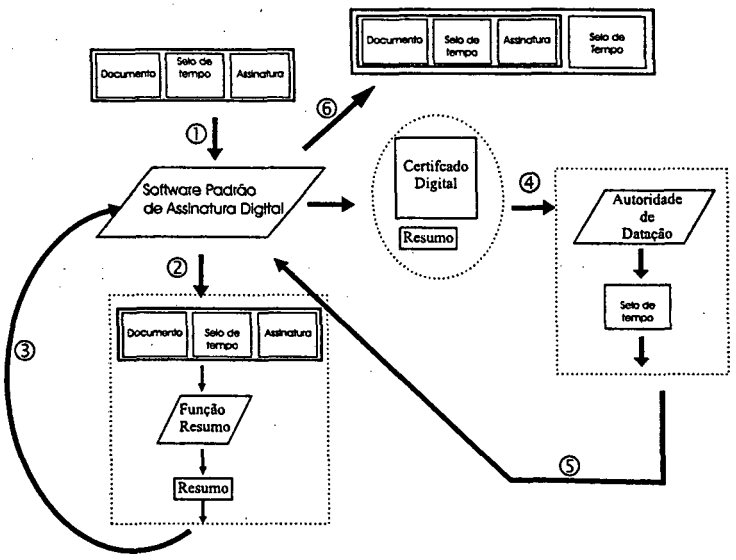

Figura 6.6: Software Padrão de Assinatura Digital - etapa 2: Atividades do SPAD para determinar o intervalo de tempo da assinatura digital.

Assim com o tempo adquirido na etapa 1, juntamente com tempo da etapa 2, o documento passa a estar assinado digitalmente e com os atributos de verificação do tempo de ocorrência da geração da assinatura. O formato apresentado por este documento nesta fase é ilustrado na figura 6.7.

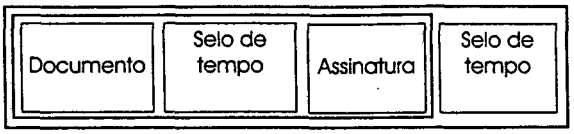

Figura 6.7: Documento com assinatura digital: Formato do documento assinado e com intervalo de tempo da assinatura após a etapa 2 do SPAD.

O atributo de selo de tempo serve também para comprovar a existência do documento em determinado momento, servindo de garantia ao receptor do documento como uma prova contra o repúdio por parte do signatário.

Na etapa 3, a última etapa da geração da assinatura, o SPAD reúne as informações úteis para conferência posterior do documento e prepara o documento para habilitá-lo ao armazenamento por tempo indeterminado na IARSDE, conforme mostra figura 6.8.

Nesta etapa a AD consulta a AGT para verificar a data de validade da tecnologia utilizada para realizar a assinatura e adiciona o estado do certificado na listas de certificados revogados naquele momento.

E o formato final, para padrão dos documentos eletrônicos assinados, denominado FADEAD (Formato Avançado de Documentos Eletrônicos com Assinatura Digital), gerados pelo software padrão de assinatura digital é ilustrado na figura 6.9

O campo de garantia de tecnologia, contém a data com a previsão da expiração da eficácia da tecnologia utilizada no processo de assinatura. Esse atributo indica a data de renovação desta tecnologia.

E o último campo, tem como função adicionar ao documento um conjunto de dados de referência para dar suporte à validação da assinatura e facilitar o processo do documento referente ao caminho de certificação e estado do certificado nas LCR's.

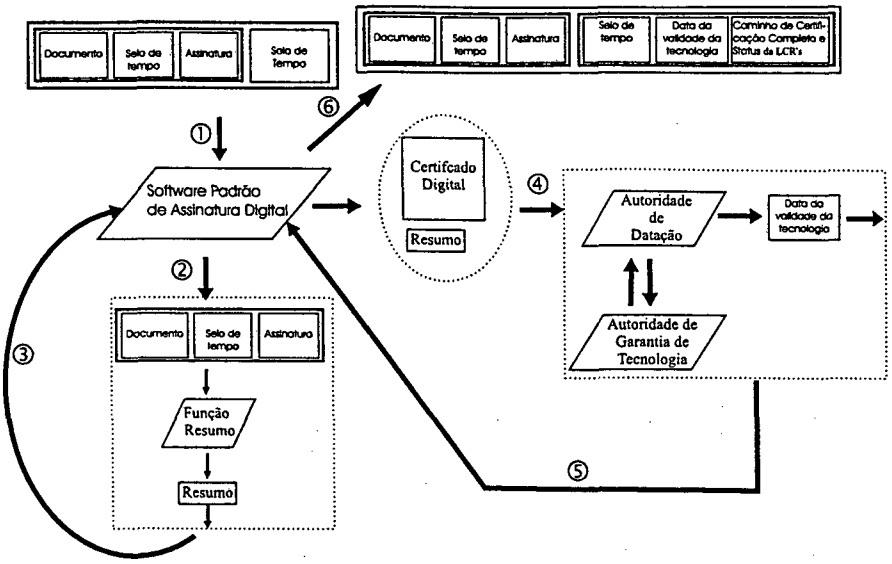

Figura 6.8: Software Padrão de Assinatura Digital - etapa 3: Fase final do SPAD para gerar a assinatura digital com atributos para garantir a renovação da tecnologia desta.

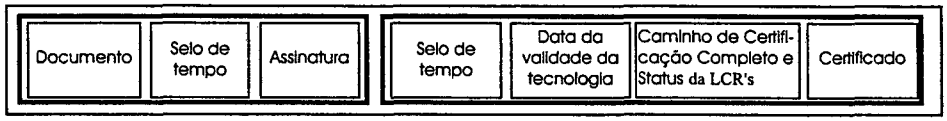

Figura 6.9: Formato Avançado de Documentos Eletrônicos com Assinatura Digital - FADEAD

6.4 Autoridade de Gerenciamento de Documentos Eletrônicos -AGDDE

Nesta seção é apresentada a proposta da autoridade de gerenciamento de documento eletrônicos da IARSDE.

A AGDDE tem como principal função a organização dos documentos na infra-estrutura, para o armazenamento e recuperação dos documentos.

Porém a maior parte do processo de gestão da IARSDE é de responsabilidade da AGDDE. Todas as principais atividades realizadas sob o documento eletrônico são geridos pela AGDDE, como o recebimento e identificação do documento, renovação da tecnologia e entrega do documento.

As subseções seguintes apresentam cada funcionalidade das atividades realizadas pela AGDDE.

6.4.1 Armazenamento seguro baseado na dispersão das informação

Ao longo do tempo, diferentes mídias foram utilizadas para armazenar informações, sejam elas o papel, microfilme, mídias magnéticas ou mídias ópticas, cada uma caracterizada por diferentes capacidades e formas de preservação dos dados.

Devido a existência dos documentos estarem diretamente ligados ao meio físico que os suportam é muito importante analisar o tempo que cada forma apresenta de segurança, e os fatores físicos dos quais são dependentes. A vida útil de um arquivo em mídia ópticas pode variar de 30 a 100 anos, um tempo considerável se comparado as mídias magnéticas que apresentam menos de 5 anos.

O modelo de preservação dos documentos eletrônicos por longo período de tempo apresentado por Ghonaimy [GHO 97], cita as principais tecnologias existentes e realiza comparações de modo a verificar a mais eficiente. Porém concentrar o armazenamento em um tipo específico de mídia pode reduzir o tempo de garantia da informação, pois a recuperação dos dados fica dependente da tecnologia existente no período de geração da informação. Por exemplo, há alguns anos um meio comum de armazenagem dos dados eram os disquetes de 5,25 polegadas, porém nos dias atuais, seria uma tarefa extremamente complicada a recuperação de dados que encontram-se nesses meios; seja pela dificuldade em encontrar o hardware para leitura, ou o software que permitisse a tradução das informações.

Uma alternativa para tratamento deste problema é a utilização do Algoritmo de Dispersão da Informação, apresentado por Rabin [RAB 89] que distribui a informação em n pedaços entre m servidores tal que a recuperação da informação seja possível até mesmo na presença de $t < m$ servidores inativos.

A noção de dispersão da informação foi introduzida por Rabin [RAB 89] com a proposta do IDA - Information Dispersal Algorithm. Esta técnica possui propriedades atraentes, como a permisão de uma parte no sistema na recuperação da infor-

mação distribuída (se comunicando com o suporte de partes), não requerendo uma autoridade centralizada. Entretanto a combinação de muitas propriedades desejáveis atinge um limite de tipo de falhas contra a robustez do algoritmo.

O **SIDA** - Secure Information Dispersal problem/algorithm [GAR 97a] é um mecanismo com o objetivo de reconstruir a informação quando ocorrem muitas faltas gerais. Este mecanismo pode tolerar os servidores maliciosos que podem intencionalmente modificar suas partes da informação, e também espaço otimizado (assintótico).

A Autoridade de Gerenciamento de Depósitos de Documentos Eletrônicos (**AGDDE**), deve trabalhar com o conceito de dispersão da informação. Dentre as diversas propostas existentes consultadas escolheu-se a proposta de Garay [GAR 97a].

Garay baseia-se no modelo de dispersão da informação, provendo algoritmos de armazenamento e recuperação da informação, porém adicionando fatores de garantia dos direitos de reprodução, distribuição e autoria dos documentos eletrônicos.

A proposta de armazenamento e recuperação de informação na IARSDE, pode ser firmada na proposta de Garay, mas apenas para a dispersão da informação. São necessários estudos adicionais sobre outras técnicas que atribuam a IARSDE requisitos dos quais faz uso, como o provimento de recibo de entrega dos documentos, com o objetivo de prover uma forma de controle aos usuários dos documentos submetidos; diferentes tipos de acesso, para possibilitar ao submissor do documento a opção da manutenção em modo público ou restrito. Essas e outras funcionalidades adicionais que se fazem necessárias são contextualizadas dentro dos temas das seções seguintes.

6.4.2 Submissão dos documentos

Os documentos submetidos à IARSDE para o armazenamento recebem uma identificação única, controlada pela AGDDE, para garantir os itens básicos de localização e recuperação. A identificação é composta pelos seguintes atributos:

Identificação do proprietário: são os mesmos existentes na identificação do certificado;

Modo de acesso: define a política de acesso e recuperação do documento;

Código de Controle: este é um campo numérico e seqüencial, com a função de identificação única do documento na infra-estrutura.

O submissor do documento deve possuir um certificado digital para que possa ser realizada a identificação do proprietário. Esta identificação consiste de um cabeçalho que é anexado ao documento, como sua identificação exclusiva dentro da IARSDE.

A necessidade de um certificado digital para identificação do proprietário, ao primeiro instante poderia ser considerado uma informação desnecessária, uma vez que o documento já possui o certificado do signatário no documento. Porém, mesmo que o documento gerado pelo SPAD possua as informações do signatário, o proprietário do documento necessariamente não será o mesmo que o signatário do documento.

Um exemplo fácil de visualizar esta situação é o caso do credor de uma nota promissória desejar manter o documento na infra-estrutura e recuperá-lo no vencimento. Ele será o proprietário do documento e terá total controle sobre ele, não podendo o signatário, cujo certificado está incluso no documento, interferir neste processo.

Na entrega do documento o proprietário define o modo de acesso ao documento na AGDDE. Existem três modos disponíveis:

Público: qualquer usuário pode acessar e realizar download do documento;

Restrito: o documento fica acessível somente ao proprietário e aos integrantes da lista de acesso definida por ele.

Privado: somente o proprietário pode ter acesso ao documento.

O modo de acesso restrito permite ao proprietário cadastrar em uma lista de acesso pessoas ou instituições para os quais os documentos seja acessível. Os dados para cadastramento dessas pessoas e/ou instituições são os mesmos do proprietário.

O código de controle é gerenciado pela AGDDE, o qual é composto por duas partes: seqüência de documentos e grupo. A seqüência de documentos equivale à quantidade de documentos recebidos pela infra-estrutura e o segundo item é o grupo (seção 6.4.3), o qual o documento será integrante.

Após o cabeçalho preenchido, a AGDDE gera um resumo desses dados e envia o a AD com o objetivo de reter prova do momento do registro do recebimento do documento . A figura 6.10 apresenta o formato do documento.

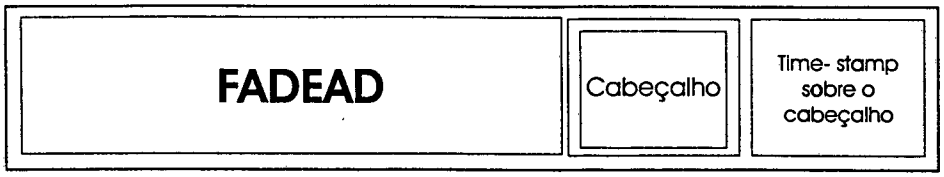

Figura 6.10: Documento com identificação da AGDDE: documento assinado com o software de geração de assinatura digital (SPAD), com identificação exclusiva na IARSDE.

6.4.3 Organização dos documentos

Para otimização dos procedimentos realizados pela infra-estrutura, os documentos devem ser mantidos de forma que apresentem uma fácil administração, segurança e confiabilidade. No processo confiado à AGDDE, todos os itens citados estão relacionados aos procedimentos e variáveis adotados em relação à organização dos documentos, controle de acesso, modo e freqüência de reassinatura.

Todos estes itens devem também ser passíveis de auditoria, de forma a garantir a credibilidade a IARSDE.

Assim a AGDDE adota o conceito de grupo para organização dos documentos com o objetivo de maximizar a performance dos processos executados pelas autoridades integrantes da infra-estrutura e facilitar sua gestão.

O registro e organização dos documentos obedecem à ordem temporal de entrega à IARSDE. A organização dos grupos também obedecem essa ordem, porém como a quantidade de documentos submetidos não apresentará uma forma linear, conforme pode ser observado no gráfico ilustrado na figura 6.11, o qual apresenta um exemplo de demanda de documentos, a IARSDE deve criar regras para formação dos grupos.

A definição de grupo na IARSDE, refere-se a uma quantidade de documentos ligados a uma identificação única, os quais são armazenados de forma que os atributos do grupo seja comum a todos os elementos pertencentes a este grupo.

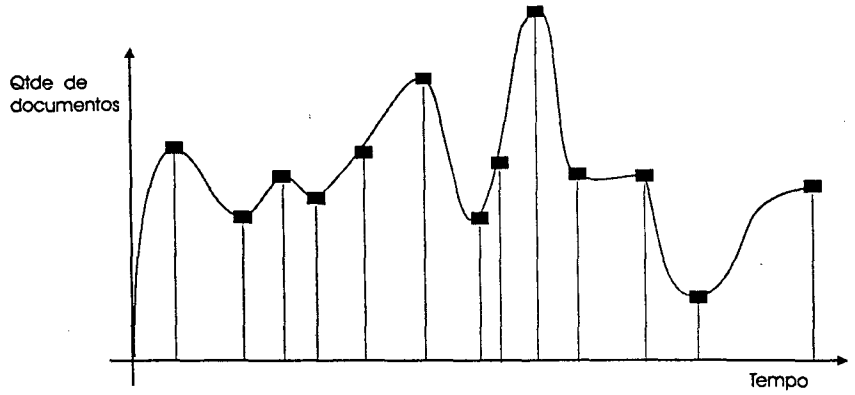

Figura 6.11: Gráfico da submissão de documentos à IARSDE: exemplo ilustrativo da quantidade de documentos submetidos a IARSDE em determinado período de tempo.

O volume de documentos recebidos pela IARSDE apresentará um gráfico ascendente e cumulativo, conforme fig 6.12.

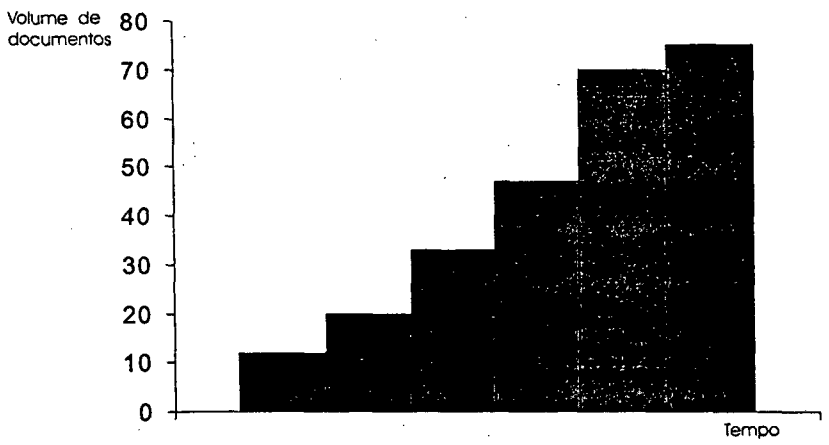

Figura 6.12: Gráfico cumulativo dos documentos submetidos à IARSDE: exemplo demonstrativo do recebimento de documentos pela IARSDE.

Os fatores de construção dos grupos são: tamanho, quantidade de documentos e tempo. Isto é baseado em três fatores controlados simultaneamente e finalização do grupo ocorre quando qualquer um dos fatores for atingido.

A determinação do tamanho do grupo deve considerar principalmente

os recursos computacionais disponíveis. A escolha de grupos muito grandes pode tornar o processo de reassinatura um procedimento lento, de grande consumo de recursos ou até mesmo ser inviabilizado. Entretanto a constituição de grupos muito pequenos gera trabalho desnecessário, pois a AGDDE e AD terão que realizar procedimentos repetidas vezes, os quais poderiam ser em uma única etapa.

Assumindo que os documentos submetidos sejam D e G o grupo formado, um grupo é definido da seguinte forma:

$$G = \sum_{i=1}^{n} tamanho\ de\ D_i \tag{6.1}$$

Os grupos definidos baseado no tamanho podem ser compostos por diferentes quantidades de documentos, variando de acordo com o tamanho e a ordem em que cada documento é submetido. Um exemplo da distribuição dos documentos é apresentado na figura 6.13. Apesar do atributo de formação do grupo ser o tamanho, eles não serão iguais, pois mesmo que o grupo não tenha alcançado o tamanho estipulado e o próximo documento ultrapasse esse valor, o grupo será fechado e este documento será alocado no próximo grupo.

O segundo fator de construção de grupos baseia-se na quantidade de documentos e está relacionado a facilidade de gerenciamento destes na infra-estrutura.

Se a formação de um grupo for baseado apenas no tamanho (o 1 fator de determinação de um grupo), e fossem submetidos em um dado momento, muitos documentos pequenos consecutivamente, este grupo seria o resultado de um acúmulo muito grande de documentos. Isto ocasionaria grupos de documentos com muitos elementos podendo dificultar a gestão dos mesmos, pois a localização pode ser comprometida pelo tempo de busca dentro do grupo.

A identificação e posterior localização de cada elemento pertencente a este grupo seria mais complexa, devido ao um grande número de documentos. Neste caso a composição do grupo seria definida por:

$$G = \sum_{i=1}^{n} quantidade\ de\ D_i \tag{6.2}$$

O terceiro parâmetro para formação do grupo diz respeito ao aspecto temporal. Se for considerado apenas os fatores tamanho e quantidade de documentos, a formação de um grupo pode demorar muito tempo, seja por não alcançar o tamanho suficiente, ou quantidade de documentos. Pois se for muito espaçado o recebimento de documentos poderá ocorrer um longo período do grupo em formação, o que pode comprometer alguns atributos do documento. Um exemplo é o caso da submissão de um documento com a data de validade da tecnologia próxima do vencimento, e caso o grupo leve muito tempo para ser formado, o prazo expirará sem a renovação da tecnologia, comprometendo a sua integridade.

A função dada por este parâmetro é definida por:

$$G = \sum_{i=0}^{tempo} D_i \tag{6.3}$$

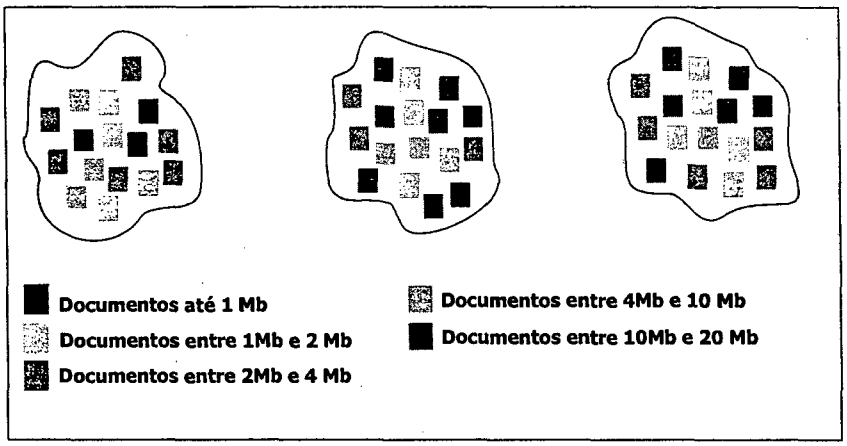

Figura 6.13: Heterogeneidade dos grupos: exemplos de grupos criados pela AGDDE, com o objetivo de ilustrar a diferença de tamanhos e quantidades de documentos de cada grupo.

Pela composição dos grupos ser determinada por três fatores distintos e simultâneos, os grupos poderão apresentar variações quanto ao seu tamanho e quantidade de documentos, conforme a figura 6.13 ilustra um exemplo.

A definição dos fatores de composição do grupo não precisam ser fixos, podem sofrer alterações com o tempo, conforme a conveniência da IARSDE.

Depois da constituição do grupo, a AGDDE empacota os documentos do grupo e gera uma identificação única, o qual recebe os seguintes identificadores:

número do grupo: identificação do grupo;

componentes do grupo: número do código de controle do documento;

Esses campos identificam o grupo na AGDDE para gestão do armazenamento e recuperação de documentos. Os documentos integrantes do grupo são listados no campo *componentes do grupo*, onde consta a identificação única do documento (código de controle recebido no momento da submissão do documento à IARSDE).

Além dos campos de identificação o cabeçalho do grupo é constituído pelos campos:

- data de validade da tecnologia - 1 (DVT-1);
- assinatura digital da IARSDE;
- data de validade da tecnologia - 2 (DVT-2);

A *data de validade de tecnologia -1* é o atributo semelhante ao existente na identificação de cada documento, porém no contexto de grupo, a data de validade de tecnologia a ser inclusa deve manter a integridade individual de todos os documento pertencentes ao grupo.

Na maior parte dos grupos de documentos formandos, seus elementos não fizeram uso da mesma tecnologia para realizar a assinatura, conseqüentemente, as datas de validade da tecnologia poderão ser divergentes. Assim para a IARSDE atribuir ao campo DVT-1 um valor que atenda todos os documentos, a AGDDE verifica a data mais próxima, ou seja o vencimento da tecnologia mais recente entre os documentos e assume como a data de validade de tecnologia do grupo. Este procedimento pode ser verificado através do exemplo ilustrado na figura 6.14.

A *assinatura digital da IARSDE* é realizada para assegurar a garantia da autoria da formação do grupo. A AGDDE provê a assinatura do grupo através do resumo

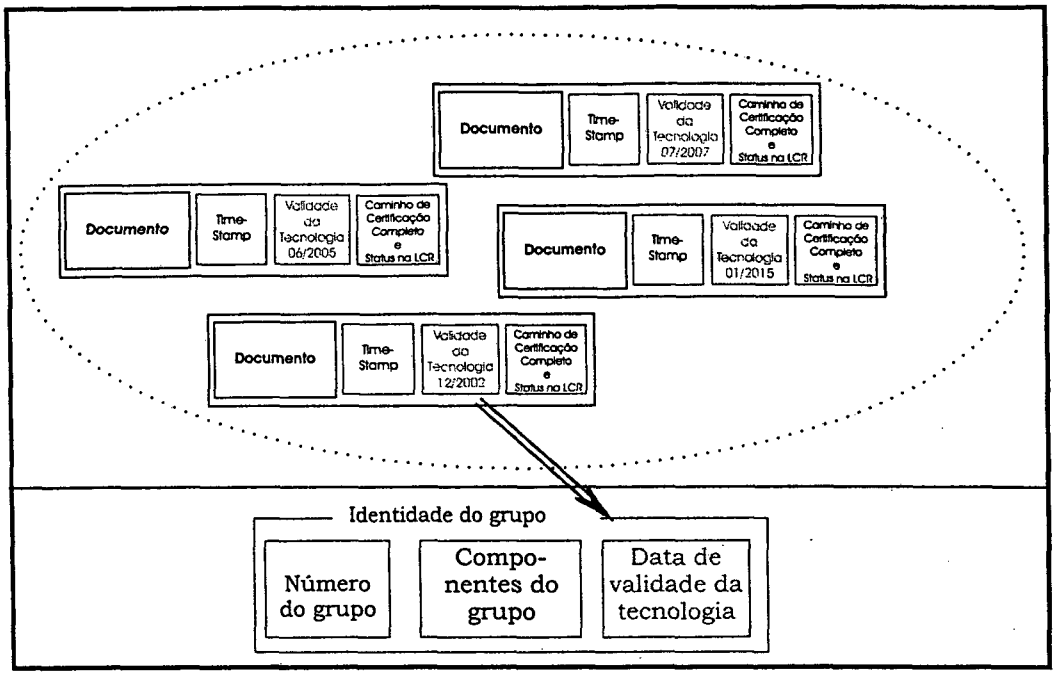

Figura 6.14: Data de validade de tecnologia do grupo: Processo de atribuição ao grupo da validade da tecnologia na submissão do documento a infra-estrutura

gerado do conjunto de todos os documentos do grupo. E o último campo do cabeçalho DVT-2 é assumido com a data de vencimento desta tecnologia.

O formato do grupo é ilustrado na figura 6.15.

6.4.4 Consulta e Comprovante de Manutenção do Documento

Os documentos mantidos na IARSDE devem estar disponíveis ao usuário, mas sempre obedecendo a regra de acesso informada na submissão do documento. A forma de acesso é disponibilizada de duas formas: consulta e comprovante de manutenção.

Na consulta, o usuário tem apenas acesso aos dados do documento, mas nenhuma informação anexa da garantia da integridade temporal. Esse usuário pode confiar que o conteúdo dos dados é o mesmo do documento original, ou seja, na integridade dos dados, mas este documento não possui provas desse atributo (assinatura digital efetu-

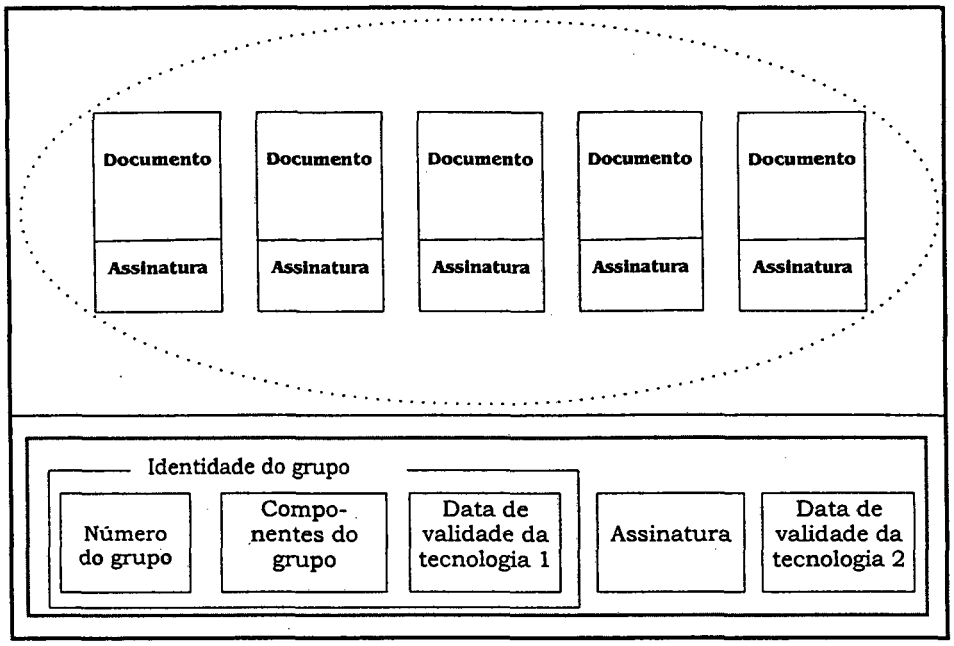

Figura 6.15: Formato do grupo de documentos: Estrutura e atributos do grupo de documentos na IARSDE.

ada pela IARSDE), garantindo que este documento foi mantido de forma regular, para os casos que a tecnologia do documento original já esteja comprometida.

Esta forma de disponibilização é mais rápida para acessar os dados, uma vez que a IARSDE tem como função apenas a verificação de acesso e localização do documento.

O acesso para obter o comprovante de manutenção do documento retorna ao solicitante, uma cópia do documento com a assinatura original acrescida do cabeçalho de identificação e assina todos esses dados com o certificado digital da IARSDE em atividade. Esta assinatura assegura que o documento foi mantido de íntegra e que sua tecnologia foi atualizada periodicamente sem a ocorrência de períodos de vulnerabilidades a fraudes.

Nas solicitações de acesso e recuperação de documentos no modo restrito ou privado, o solicitante deve submeter seu certificado para a AGDDE verificar se este usuário é autorizado a ter acesso a esta informação.

Como no modo privado só existe um usuário autorizado ao acesso do documento a AGDDE verifica as informações do certificado com o cabeçalho do documento. Já o modo restrito a conferência é estendida à lista de acesso.

Se as informações conferirem, a AGDDE cifra o documento com a chave pública do certificado apresentado e envia o documento ao solicitante.

Dessa forma o controle de acesso ao documento é garantido, pois tentativas maliciosas são contornadas através da cifragem do documento antes da entrega ao solicitante. Se um elemento malicioso apresentar o certificado de outro usuário, que seja proprietário do documento ou esteja na lista de acesso, ele pode receber o documento, porém não conseguirá abri-lo, pois não possui a chave privada para tal.

O certificado apresentado para identificação não precisa ser o mesmo que da submissão do documento e provavelmente não o será, pois a maioria dos certificados apresentam tempo validade de um ano, e os documentos armazenados podem permanecer por tempo indeterminado na IARSDE, inclusive depois da revogação de muitos certificados do proprietário do documento. Entretanto, como nos campos de identificação do usuário do certificado, as informações serão as mesmas em diferentes certificados que vir a possuir, os usuários autorizados poderão ser verificados.

6.5 Reassinatura

O tempo da integridade do documento eletrônico está associado a tecnologia utilizada para garantir sua autoria e autenticidade (assinatura digital). A fig 6.16 apresenta a linha temporal do certificado.

Conforme pode-se observar na figura 6.16, somente as assinaturas efetivadas entre t_2 e t_3 poderão ser consideradas válidas. Porém mesmo sendo realizadas em um período válido, essa assinatura tem o tempo de garantia da integridade limitado, pois no instante que ocorre o comprometimento da tecnologia, significa que existem técnicas ou poder computacional que possam forjar uma assinatura correspondente a este certificado. Entretanto o tempo de validade do documento eletrônico não deve estar fixa a este fator, sendo necessária a criação de métodos que permitam a atualização desse item.

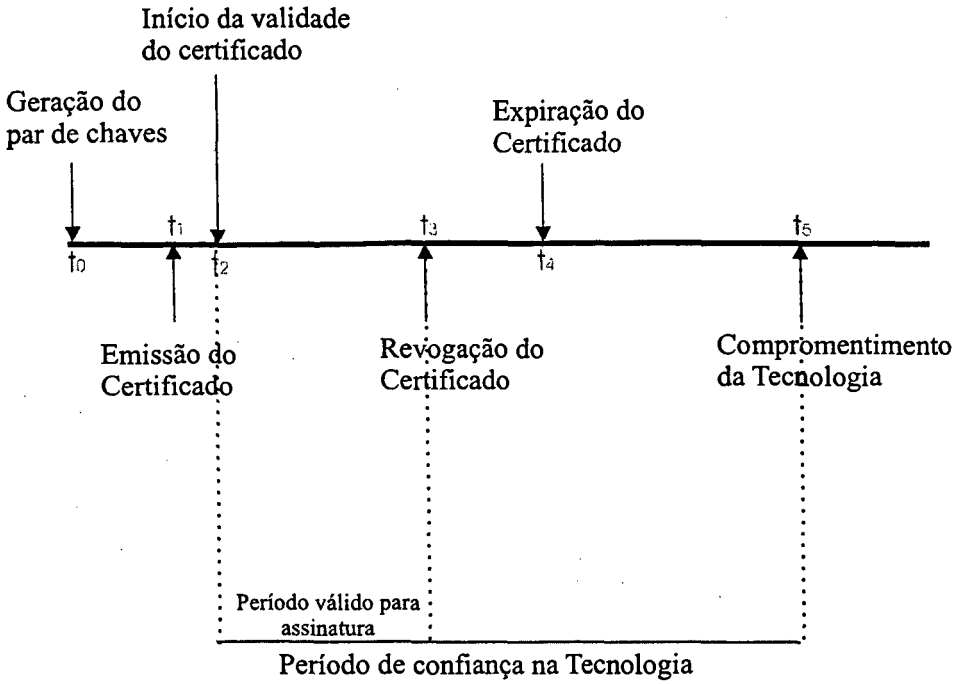

Figura 6.16: Descrição da linha temporal de um Certificado Digital: t_0 - geração do par de chaves pública e privada pelo usuário; t_1 - emissão do certificado pela AC; t_2 - início da validade do certificado; t_3 - revogação do certificado por solicitação do usuário; t_4 - expiração da validade do certificado determinado na emissão; t_5 - comprometimento da tecnologia, por criptoanálise ou poder computacional.

O controle desse aspecto é de responsabilidade da AGDDE. A verificação e atualização da tecnologia empregada para assinatura do documento deve ser renovada antes do seu comprometimento para reter provas de seu valor legal.

No vencimento da tecnologia mantido nos campos de identificação do documento, a AGDDE dispara o processo adequado para conferir a atualização da tecnologia, denominado reassinatura.

O conceito de reassinatura do documento na IARSDE, consiste na geração de uma nova assinatura, com uma tecnologia atual e mais robusta, ou seja, é calculado o resumo do documento completo (com a assinatura inclusa) e submetido à AD para adicionar um novo selo de tempo e informações da validade da tecnologia utilizada.

Esse processo é repetido todas as vezes em que a tecnologia expirar,

sendo que o documento é encapsulado novamente com todas as assinaturas anexadas anteriormente, como mostra figura 6.17, para que seja possível verificar se a ocorrência da atualização da tecnologia foi realizada em tempo hábil.

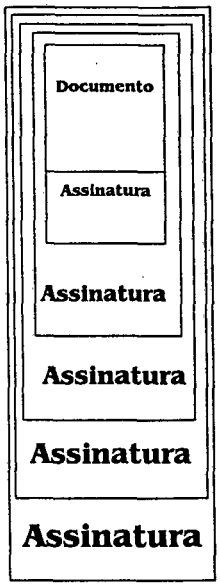

Figura 6.17: Documento reassinado: documento submetido ao processo de assinatura enumeras vezes

A AGDDE mantém a estrutura de grupos para gerenciamento dos documentos. Então todo o processo referente à reassinatura de documentos é aplicado sobre grupo.

O processo de reassinatura do grupo consiste no cálculo do resumo do grupo, em toda a estrutura, incluindo o cabeçalho. Este resumo é assinado utilizando o certificado da IARSDE e é enviado a AD, a qual retorna o recibo da protocolação e data de validade da tecnologia.

Porém, apesar de todos os procedimentos realizados pela AGT, uma tecnologia pode ser quebrada muito antes da previsão de comprometimento. Neste caso a assinatura tornaria-se fraca e passível de personalização, e a integridade destes documentos seria comprometida.

Neste sentido a AGDDE garante a integridade dos documentos através

da utilização simultânea de duas tecnologias para cada grupo de documento. Na identificação do grupo do documento, como a IARSDE assina o grupo, este tem como garantia essa assinatura, e a assinatura do documento, pois ambas não estão comprometidas. Assim deste a formação do grupo os documentos passam a contar com a segurança de duas tecnologias.

O processo de reassinatura também garante esse nível de confiabilidade através do emprego de duas assinaturas ao grupo, utilizando duas tecnologias distintas.

Para isso, o resumo do documento é gerado duas vezes, cada um com uma função resumo diferente e cifrado com a chave privada da IARSDE utilizando também duas tecnologias diferentes. Em seguida estas assinaturas são encaminhadas a AD.

Desta forma o grupo passa a ter duas tecnologias distintas para manutenção dos atributos dos documento. Conseqüentemente, terá duas datas de validade de tecnologia diferentes. A AGDDE assume como data para o processo de reassinatura, a mais próxima. Porém caso ocorra o comprometimento de qualquer uma delas antes do prazo previsto, a AGDDE dispara o processo de reassinatura e atribui duas novas tecnologias de assinatura.

6.6 AGT - Autoridade de Garantia de Tecnologia

A Autoridade de Garantia de Tecnologia é o elemento responsável pela disponibilização de listas com dados sobre a previsão do comprometimento da tecnologia utilizada para a datação e/ou assinatura digital, seja pela existência de poder computacional para quebra do algoritmo criptográfico, ou por ataques de criptoanálise.

A tarefa de mensurar a eficácia da proteção das informações depende de uma variedade de itens como o tamanho das chaves, projeto do protocolo e seleção das senhas. Cada um desses itens é igualmente importante: se uma chave for muito pequena, o protocolo for mal projetado ou se a senha for selecionada e/ou protegida de forma deficiente, a proteção está comprometida e o acesso impróprio pode ser obtido [LEN 99].

Os cálculos dessas previsões podem basear-se nos seguintes itens [LEN 99]:

- Extensão de vida: tempo previsto que a proteção seja eficaz;
- Margem de segurança: grau aceitável de insegurança em relação ao sucesso de ataque;
- Ambiente computacional: expectativa de mudança nos recursos computacionais;
- Criptoanálise: expectativa de desenvolvimento da criptoanálise.

Para garantir que as listas geradas e disponibilizadas apresentam-se próximas a realidade, a AGT deve estar atenta as diversas pesquisas relacionadas as tecnologias.

As atualizações devem ser constantes e realizadas num tempo fixo determinado, e observando o surgimento de novos tamanhos de chaves para um algoritmo já existente ou a apresentação de uma nova tecnologia, e principalmente casos de comprometimento de qualquer tecnologia já constante na lista, antes do prazo previsto.

As listas de informação da validade de tecnologias mantidas pela **AGT** devem sempre manter-se disponíveis para consulta. Não somente a AD pode fazer solicitação de consultas à lista, como qualquer entidade pode obter informações sobre determinada tecnologia.

O processo será diferente para esses dois tipos de consulta, pois a AD quando enviar o documento à AGT, esta verificará qual foi a tecnologia utilizada, consultará suas listas e enviará a data do cálculo mais recente. Nas consultas de usuários à AGT, poderão ser pesquisados o histórico da tecnologia, onde serão retornadas todas as previsões de datas de comprometimento, e suas alterações.

Além da manutenção das datas de previsões de comprometimento, a AGT mantém armazenadas todas as tecnologias constantes na sua lista, pois se a conferência de uma assinatura necessitar de uma tecnologia comprometida há vários anos e precisar encontrá-la, provavelmente isto seria uma tarefa muito difícil e trabalhosa. Então a AGT também oferece serviços de disponibilidade das tecnologias.

Eventuais tecnologias serão quebradas antes do prazo previsto pela AGT, provavelmente através de técnicas de criptoanálise. Se isto ocorrer, os documentos manti-

dos por esta tecnologia se tornarão vulneráveis até a data de atualização estimada anteriormente. Para que isso não ocorra, a AGT tem como função avisar a AGDDE esses fatos. A **AGT**, envia um aviso a **AGDDE** informando que a tecnologia encontra-se comprometida para que esta atualize novamente os documentos assinados com outra tecnologia.

6.7 Autoridade de Datação

Existem dois tipos de técnicas de datação: aquelas que trabalham com uma terceira entidade confiável (Autoridade de Datação - AD); e aquelas que são baseadas no conceito de confiança distribuída [PAS 01]. Técnicas baseadas em AD confiam na imparcialidade da entidade encarregada da datação. Já a técnica baseada na confiança distribuída consiste em datar e assinar o documento por vários elementos de um grupo de modo a convencer o verificador que não se poderia corromper todos os elementos simultaneamente.

Um método eficiente de datação deve atender os seguintes requisitos de segurança [HAB 91]:

- Privacidade: Ninguém além do cliente pode ter acesso ao conteúdo do documento;
- Canal de comunicação e armazenamento: Deve ser prático datar o documento independentemente de seu tamanho;
- Erro na comunicação: Deve-se garantir a integridade dos dados e a operação ininterrupta do serviço de datação;
- Anonimato: Deve-se garantir o anonimato do cliente;
- Confiança: Deve-se garantir que um documento será datado com a data e hora correta;

As técnicas baseadas em AD são mais adequadas do que as técnicas baseadas em confiança distribuída para o atendimento destes requisitos uma vez que existem métodos que podem garantir de forma incontestável a confiança da AD.

A primeira maneira prática de datar um documento é enviá-lo para uma AD. A AD acrescenta data e hora no documento, armazena uma cópia que será utilizada em caso de disputa e devolve um recibo indicando que o documento foi datado. Este não é um bom procedimento já que não atende aos requisitos de privacidade, uma vez que a AD fica conhecendo o documento; e o uso do canal de comunicação e armazenamento pode ser muito exigido, uma vez que todo o documento deve ser transmitido e armazenado. Este problema será ainda maior caso o documento seja muito grande ou exista muitos documentos a serem datados.

Para resolver este problema pode-se utilizar o resumo do documento, conhecido como hash. O resumo representa de forma única um documento. Assim, ao invés da transmissão do documento, é enviado o resumo do documento, e dessa forma ocorre o atendimento dos requisitos de privacidade, uso do canal de comunicação e espaço de armazenamento.

Outro aperfeiçoamento que pode ser realizado é adicionar assinatura digital ao esquema, ou seja, quando o resumo do documento chega para ser datado, a AD anexa data e hora ao resumo, assina e o envia ao cliente do serviço. O cliente por sua vez verifica a assinatura e tem certeza que o resumo que ele enviou foi realmente o resumo que foi enviado para a AD. Com isso garante-se também o requisito de erro na comunicação.

Existem várias formas de resolver o requisito de anonimato. O atendimento do anonimato não invalida o cumprimento dos outros requisitos de segurança. O anonimato pode ser visto como um complemento desejável, existindo muitas situações onde não há a sua necessidade.

O requisito de confiança pode ser atendido se a AD é considerada confiável. Isso pode ser obtido, na prática, tendo-se um equipamento lacrado e passível de auditoria. Contudo, o lacre e a auditoria implicam em custos e possibilidade de fraudes, provocando uma desconfiança por parte do cliente. Na realidade, o uso de auditoria só transfere a necessidade de confiança a uma quarta entidade, neste caso o auditor. O ideal seria que a AD não pudesse ser maliciosa, mesmo que seu administrador o fosse. Isso já é possível com a utilização de alguns dos métodos.

Estes métodos levam em consideração a questão temporal, ou seja, como o documento recebe a data e hora. Ela pode ser absoluta ou relativa. A autenticação temporal absoluta contém informações de data e hora igual a usada no mundo real. Já a autenticação temporal relativa contém informações que somente verificam se um documento foi datado antes ou depois de um outro documento.

Os dois esquemas temporais podem ser usados para se datar documentos, mas o esquema absoluto pressupõe que a AD seja uma entidade confiável. Para o esquema relativo não é necessária a existência de entidade confiável, pois existem mecanismos que garantem que mesmo que a AD ou seu administrador queiram ser maliciosos, o documento sempre será datado com data e hora corretas.

O problema da confiança na AD pode ser tratado através da utilização do encadeamento dos resumos dos documentos protocolados [PAS 01].

A confiabilidade da AD é de extrema importância, pois se esse fator inexistir, a integridade da infra-estrutura pode ser comprometida. Desde a identificação dos documentos até o processo de entrega do documento, a AD que introduz a segurança contra possibilidades de alterações sem detecção, na estrutura dos dados depois de submetidos e armazenados.

6.8 Auditoria

O processo de auditoria consiste no ato de vistoriar com o propósito de constatar. Este é um elemento importante na conjuntura de um sistema, pois pode apontar falhas e/ou possíveis fraudes, como também adicionar garantia de confiabilidade. Com este propósito a infra-estrutura provê formas para que esta tarefa seja possível.

A garantia da validade do documento eletrônico por longo período de tempo proporcionada pela IARSDE está diretamente relacionada à confiabilidade atribuída a ela. Uma vez que os documentos ao serem retirados da infra-estrutura são assinados com o certificado da IARSDE, a garantia de que todos os processos ocorreram, e no seu devido tempo é dada por esta assinatura.

Porém não existem indícios no documento entregue pela IARSDE que

possibilitem a verificação dos procedimentos adotados durante o tempo de manutenção do documento na infra-estrutura. Então a confiança é depositada somente na assinatura da IARSDE.

Mas surgem questionamentos de como ter a certeza de que os procedimentos necessários foram tomados e no tempo correto. E se as autoridades que compõem a infra-estrutura são realmente confiáveis.

A garantia dos processos das atividades na IARSDE devem estar ligados ao tempo em que foram realizados, pois conforme já explicada nas seções anteriores o controle da expiração da tecnologia é dependente deste fator.

Assim a auditoria na IARSDE tem como objetivo:

- verificar a integridade de cada assinatura;
- constatar se todos os processos de reassinatura ocorreram no tempo devido;
- verificar a integridade da identificação do documento e do grupo.

A conferência destes itens é realizada através do exame das assinaturas na sua ordem cronológica, ou seja, da mais recente para a mais antiga. Por exemplo no caso de um documento que tenha sido reassinado três vezes, e portanto possui quatro assinaturas; a ordem de conferência é da quarta assinatura para a primeira, como ilustra a figura 6.18.

Conforme a assinatura é conferida nos itens de autoria e integridade da tecnologia, a data de validade da tecnologia utilizada para geração desta assinatura é consultada na AGT e comparado com o selo de tempo da assinatura, se a reassinatura ocorreu em tempo menor que a expiração a assinatura é válida. Caso contrário este documento foi submetido a atualização de tecnologia fora do tempo correto, podendo então ter sido personalizado ou sofrido alterações, uma vez que a tecnologia foi atualizada quando todas as tecnologias já encontravam-se comprometidas.

Este processo de conferência deve ser certificado em todas as assinaturas do documento. Se em alguma delas algum item falhar, os documentos relacionados a estas assinaturas não podem ser considerados válidos .

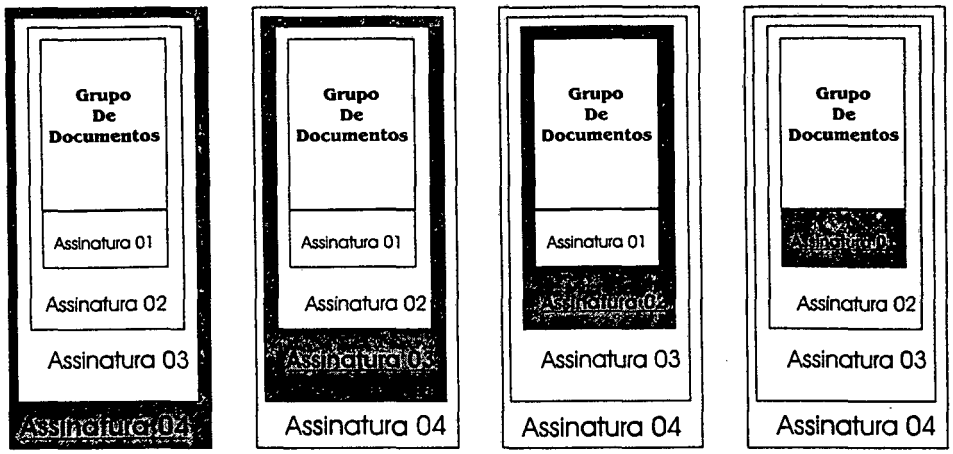

Figura 6.18: Seqüência da conferência da assinatura

A auditoria nestes itens acima garantem que o processo de reassinatura dos documentos foi realizada corretamente e garante também a integridade dos dados do documento original. Tentativas de substituição do documento original por um outro documento, teria que conseguir atender a uma cadeia de restrições imposta a cada nova assinatura.

A figura 6.19 mostra um exemplo de uma tentativa de ataque, tendo como objetivo a alteração ou substituição de um documento. Neste exemplo o documento original já passou pelo processo de atualização da tecnologia por duas vezes. Assim a primeira assinatura já encontra-se comprometida a um período de tempo razoável e portanto existe poder computacional suficiente e técnicas de criptoanálise, com os quais é possível encontrar um documento diferente do original que gere o mesmo resumo.

Se dois documentos distintos possuem o mesmo valor resumo, as assinaturas também serão iguais se for utilizada a mesma tecnologia. Assim a primeira etapa da tentativa de fraude poderia ser realizada sem grande grau de dificuldade.

Porém na segunda assinatura, a função resumo utilizada não é igual a utilizada na primeira, e conseqüentemente o resumo resultante para gerar a segunda assinatura dificilmente será igual se o documento original for substituído ou alterado. Mesmo que o resumo seja igual ao do documento original, o processo de reassinatura

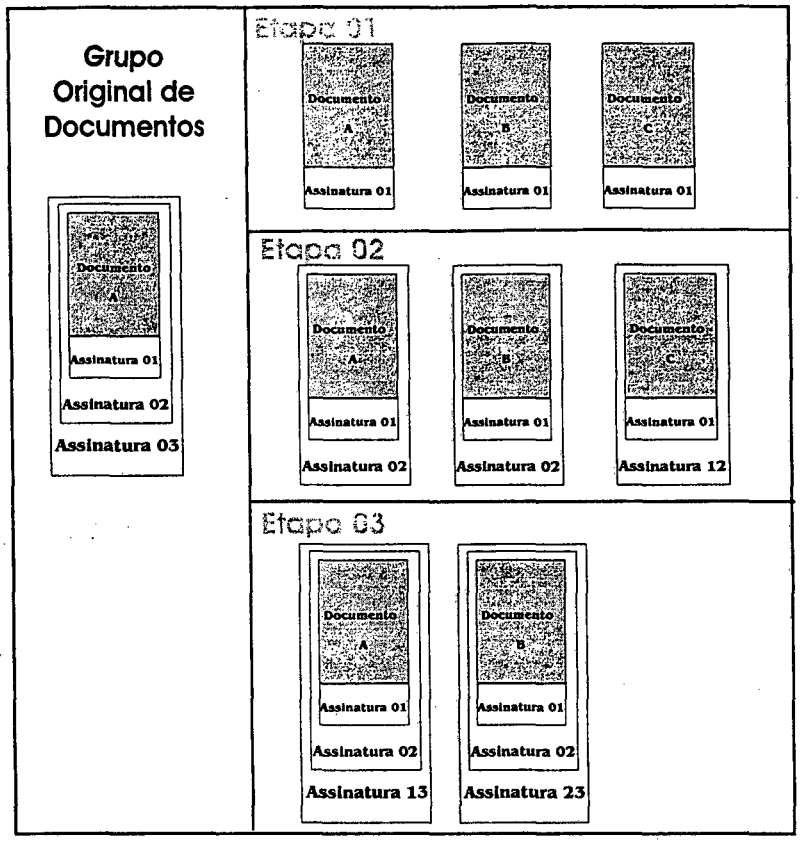

Figura 6.19: Tentativa de substituição do documento: Na etapa 1 o ataque consegue obter três documentos A, B e C que resulte na assinatura 1 do documento original. Na etapa 2 somente os documentos A e B geraram uma assinatura igual a assinatura 2 e podem ser candidatos a próxima etapa. Na etapa 3 nenhum dos documentos conseguem personalizar a assinatura 3.

calcula o resumo baseado não só no resumo da assinatura anterior, e sim no documento original e todas as assinaturas já existentes.

Assim para obter sucesso na segunda etapa, o atacante deve conseguir não só gerar um resumo igual ao da primeira assinatura, mas que esse documento assinado resulte em resumo igual ao da segunda assinatura. Entretanto como as tecnologias já encontram-se comprometidas, não podemos descartar a possibilidade de sucesso.

Para o atacante obter sucesso e conseguir finalmente completar a operação, ele deve tentar gerar uma assinatura igual a terceira assinatura. Porém esta etapa está garantido com uma tecnologia atual e portanto difícil de personalizá-la, além de que

ele teria a assinatura está encadeada as outras assinatura , assim o atacante não consegue completar todas as série do ataque.

Além da dificuldade da tecnologia atualizada e do encadeamento das tecnologias, o atacante se depara com a estrutura de grupos de documentos, mantida pela IARSDE. Pois apenas para simplificar o entendimento do ataque foi utilizado o termo documento, mas na IARSDE todo esse processo ainda teria que levar em consideração esta estrutura, o que aumentaria ainda mais o grau de dificuldade.

O outro item importante para a auditoria é a verificação da identificação do documento e do grupo para constatar se esses elementos foram submetido na ordem que possuem no seu cabeçalho e os atributos de data e hora não foram alterados. A confiabilidade dessas informações podem ser averiguados através em uma auditoria na AD [PAS 01], pois depois da submissão dos documentos ou da formação dos grupos, é gerado um resumo desses dados e submetidos a AD.

6.9 Software padrão para visualização e verificação da assinatura digital

Assim, com já discutido anteriormente, é sabido que a verificação da assinatura digital não é trivial. Ela depende da conferências de equações matemáticas, as quais mantém a ligação entre as chaves públicas e privadas. Essa conferência está relacionada a necessidade de um software que trate estes dados.

Um software para tratamento das informações de uma assinatura digital deve ser constituído de um verificador e um visualizador.

O verificador da assinatura deve verificar a autoria e integridade do documento através da conferência do resumo do documento. Este processo de conferência está descrito no capítulo 2.

Outra função do verificador é informar ao conferente a árvore de certificação do certificado do signatário, possibilitando assim a verificação do AC raiz na qual este certificado confia.

Já o visualizador tem a tarefa de reproduzir fielmente as informações contidas em um certificado digital. Este software tem como objetivo proporcionar ao receptor do documento a garantia de conferência de todas as informações necessárias para confiabilidade da identificação do signatário.

Um software de visualização de certificados digital, foi desenvolvido no Laboratório de Segurança em Computação - LABSEC, da Universidade Federal de Santa Catarina UFSC, podendo ser visto maiores detalhes no Anexo I. Este visualizador possui código fonte aberto, permitindo a análise do seu funcionamento. Este fator adiciona segurança e confiabilidade, pois os softwares com código proprietário não permite verificar se há manipulação dos dados e/ou as informações são apresentadas da forma correta.

Assim como o software para geração da assinatura digital é importante, é de grande valia também, o governo estar atento para adoção de softwares padrão que realizem o processo de verificação e visualização deste elemento. E principalmente estar atento a propostas e softwares implementados no Brasil, sem a necessidade de adoção de padrão de softwares estrangeiros o qual não é possível verificar a integridade da sua execução e nem realizar possíveis alterações necessárias.

6.10 Conclusão

A IARSDE através de suas autoridades oferece uma forma segura de armazenamento de um documento eletrônico, onde são preservados seus atributos, garantindo a validade por tempo indeterminado.

A IARSDE utiliza o conceito de grupo, para organização dos documentos. Se não fosse utilizado esta estrutura e cada documento recebesse uma identificação individual, o processo de reassinatura seria passível de verificação e a confiança neste documento não necessitaria ser depositada no processo de auditoria na IARSDE.

Isto porque o documento poderia ser entregue com toda a seqüência de assinaturas que foi submetida ao longo do tempo, e possibilitaria ao software de verificação de assinatura a conferência de cada uma delas. Porém a quantidade de ele-

mentos a serem geridos pela IARSDE aumentaria significativamente, podendo resultar num gargalo de serviços a serem executados.

A manutenção de grupos torna a segurança dos documentos ainda mais concisa, pois as tentativas de fraude de um documento resultaria no trabalho com um conjunto de documentos, aumentando a dificuldade de êxito. Por estas razões a IARSDE adota esta estrutura.

Outra proposta apresentada são as ferramentas para geração, visualização e conferência da assinatura digital. O governo brasileiro deve ater-se em verificar a importância da adoção de softwares padrão e órgãos fiscalizadores para a confiabilidade deste sistema.

Capítulo 7

Considerações Finais

O objetivo geral do trabalho foi contemplado na sua totalidade, pois a infra-estrutura proposta atende os requisitos de garantia do documento por tempo indeterminado. Esse item é assegurado através dos processos de atualização da tecnologia utilizada para assinatura do documento antes do seu comprometimento, denominado re-assinatura.

A reassinatura mantém a tecnologia atualizada, ou seja, uma que não possua técnica de criptoanálise eficiente ou poder computacional suficiente para quebrá-la em tempo hábil. Este processo de atualização faz com que as tecnologias utilizadas nos processos de assinatura anteriores, as quais já encontram-se comprometidas e consideradas fracas, fiquem encadeadas à atual. Desta forma a integridade do documento e da assinatura original são mantidos.

De acordo com objetivos específicos, na definição do documento eletrônico foram apresentadas diferentes visões de diversos juristas, até encontrar justificativas fundamentadas com as quais foi possibilitado ao documento eletrônico enquadrar-se na definição de documento sob o prisma jurídico.

Este trabalho apresentou uma revisão bibliográfica dos elementos criptográficos básicos, apresentando o funcionamento dos esquemas de assinaturas digital dando base para o estudo na análise dos requisitos dos documentos.

Assim foi constatado que para obter-se a equiparação sob ponto de vista

legal de ambas formas de documento é necessário que o documento eletrônico se adeque, e apresente no mínimo os mesmos requisitos do documento papel, visto que este já possui sua base jurídica fundamentada a muito tempo. Para isso foram analisadas as propriedades tecnológicas dos documentos eletrônicos levantando os fatores atendidos e os ainda carentes de soluções.

Com o levantamento das vantagens e desvantagens de cada forma de documento, verificou-se a perspectiva de existência de ambas as formas por longo período de tempo. Como uma simples conversão entre formatos não garante a validade jurídica dos documentos, uma proposta para manutenção deste item, utilizando a infra-estrutura existente para o documento papel é apresentada.

Dentre os requisitos analisados, o documento eletrônico não apresenta características confiáveis quanto ao aspecto temporal da sua validade.

Ainda sobre o estudo do documento eletrônico, foi constatado que alguns países já instituíram leis para que os órgãos do governo adotem o documento eletrônico, não podendo rejeitar qualquer documento por estar neste formato. O Brasil não possui nada regulamentado, mas deve ater-se a essa nova necessidade mundial.

Através do levantamento das linguagens de marcação apresentadas, nas quais apresentam-se os principais padrões de assinatura digital existentes, foi encontrado alguns trabalhos ligados a busca da manutenção da validade dos documentos eletrônicos por longo prazo. Entre as propostas encontradas, elas apenas prolongam o prazo de validade ou não apresentam forma de gestão dos procedimentos necessário, não podendo verificar se realmente alcança o resultado esperado.

De forma a complementar a proposta da IARSDE, são apresentadas propostas de ferramentas de geração e verificação da assinatura digital, com o objetivo de produzir um padrão de documento assinados que suportem o armazenamento por período inderminado.

7.1 Trabalhos Futuros

As sugestões de trabalhos futuros como uma extensão do trabalho apresentado nesta dissertação, relaciona-se ao desenvolvimento e implementação das autoridades pertencentes a infra-estrutura.

Para a implementação da Autoridade de Garantia de Tecnologia, deve observar-se diferentes propostas existentes no sentido de verificar a segurança das chaves, procurando englobar as melhores características de cada proposta. A eficácia da AGT depende não somente das estimativas de cada tecnologia, mas também da atenção dada as novas técnicas de ataques e poder computacional existente. Assim se faz necessário um estudo da melhor forma de gestão da autoridade, formas de atualização de cálculo, do direcionamento das pesquisas de criptoanálise, e atualização das pesquisas já existentes.

A implementação da Autoridade de Gerenciamento de Depósito de Documentos Eletrônicos deve observar além dos critérios operacionais impostos pela proposta da IARSDE, os fatores de segurança dos servidores contra ataques de negação de serviço, invasão e roubo de informação, os quais não foram tratados no trabalho.

Como a Autoridade de Datação já possui propostas prontas e implementadas, bastando apenas adequá-la, de forma a incluir o serviço de consulta as listas mantidas pela AGT.

Referências Bibliográficas

[BAT 01] BATISTA, H. G.; MAGRO, M. E. Cartórios investem para mudar imagem e não o perder mercado. **Valor on line**, [S.l.], outubro, 2001.

[BRA 01] BRASIL, A. B. Não repúdio: Eficácia jurídica dos negócios eletrônicos. **www.direitonaweb.com.br**, [S.l.], maio, 2001.

[CEN 98] CENADEM. Armazenamento de imagens de documentos. **Mundo da Imagem**, [S.l.], , n.26, p.3, abril, 1998.

[CHI 69] CHIOVENDA, G. **Instituições de direito processual civil**. São Paulo: Saraiva, 1969.

[COU 97] COUTINHO. **Números inteiros e criptografia RSA**. Computação e Matemática. Instituto de Matemática Pura e Aplicada, 1997.

[dA 01] DE ASSIS, A. C. K. T. A certificação digital na internet. **http://www.praetorium.com.br/artigos/internet.htm**, [S.l.], 2001.

[DB 91] DAVE BAYER, STUART HABER, W. S. S. Improving the efficiency and reliability of digital time-stamping. **Sequences91: Methods in Communication, Security, and Computer Science**, [S.l.], p.329–334, 1991.

[dH 96] DE HOLANDA, A. B. Novo dicionário da língua portuguesa. **Nova Fronteira**, [S.l.], 1996.

[DIF 76] DIFFIE, W.; HELLMAN, M. New direction in criptography. **IEEE Transactions on Information Theory**, [S.l.], November, 1976.

[ele 01] Xml advanced electronic signatures (xades). **European Telecommunications Standards Institute**, [S.l.], novembro, 2001.

[FOR 97] FORD, W.; BAUM, M. S. **Secure Eletronic Commerce**. New Jersey: Prentice-Hall, 1997.

[GAR 97a] GARAY, J. et al. Secure distributed storage and retrieval. **11th International Workshop on Distributed Algorithms**, [S.l.], p.275–289, 1997.

[GAR 97b] GARFINKEL, S.; SPAFFORD, G. **Web Security e Commerce**. 1. ed. O Reilly & Associates, Inc., 1997.

[GHO 97] GHONAIMY, M. A. R. Existing and evolving technologies for long-term information preservation and the supporting legal requirements. **Academic Press Limited**, [S.l.], p.367379, 1997.

[GOY 00] GOYA, D. H. Biometria: Diversas tecnologias permitem identificar pessoas pelas características físicas. **PC World**, [S.l.], p.54–62, agosto, 2000.

[HAB 91] HABER, S.; STORNETTA, S. How to time-stamp a digital document. **Journal of Cryptology**, [S.l.], v.3, p.99–112, 1991.

[HOU 01] HOUSLEY, R.; POLK, T. **Planning for PKI - Best Practices Guide for Deploying Puclic Key Infrastucture**. 1. ed. Wiley, 2001.

[JR 96] JR, H. T. **Curso de direito processual civil**, v.I. Rio de Janeiro: Forense, 1996.

[LEN 99] LENSTRA, A. K.; VERHEUL, E. R. Selecting cryptographic key sizes. **Crypto2000**, [S.l.], novembro, 1999.

[MAR 98] MARCACINI, A. T. R. O documento eletrônico como meio de prova. **http://members.xoom.com/marcacini/docelet.pdf**, [S.l.], Outubro, 1998.

[MAR 00] MARTINS, H. Assinaturas eletrônicas - o primeiro passo para o desenvolvimento do comércio eletrônico? **http://www.cbeji.com.br/artigos/artmarcelodeluca08102001.htm**, [S.l.], 2000.

[MIR 95] MIRABETE, J. F. **Processo Penal**. 4. ed. São Paulo: Atlas, 1995.

[NIS 93] NIST. Secure hash standard. National Institute of Standards and Technology - Department of Commerce, May, 1993. Federal information processing standards publication 180.

[NIS 94] NIST. Digital signature standard. National Institute of Standards and Technology - Department of Commerce, May, 1994. Federal information processing standards publication 186.

[PAS 01] PASQUAL, E. S. **IDDE - Uma Infra-estrutura para a Datação de Documentos Eletrônicos**. UFSC - Universidade Federal de Santa Catarina, dezembro, 2001. Dissertação de Mestrado.

[PUR 01] PUREEDGE. What is the government paperwork elimination act, and how will it impact your business ? **http://www.uwi.com/solutions/gpea/index.htm**, [S.l.], consultado em 03 de novembro de 2001.

[RAB 89] RABIN, M. Eficient dispersal of information for security, load balancing, and fault tolerance. **J. ACM**, [S.l.], p.335–348, 1989.

[RIV 78] RIVEST, R.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public key cryptosystems. **Communications of the ACM**, [S.l.], February, 1978.

[SAN 97] SANTOS, M. A. **Primeiras linhas de direito processual civil**, v.2. 18. ed. São Paulo: Saraiva, 1997. p.385.

[SCH 95] SCHNEIER, B. **Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition. 2.** ed. John Wiley and Sons, 1995.

[STA 99] STALLINGS, W. **Cryptography and Network Security**. 2. ed. Prentice Hall, 1999.

[STI 95] STINSON, D. R. **Cryptography : Theory and Practice**. CRC Press, 1995.

[TRU 97]• TRUJILLO, É. O mercosul e a documentação eletrônica. **http://www.teiajuridica.com/mercosul.htm**, [S.l.], Outubro, 1997.

Apêndice A

O Visualizador de Certificados Digitais

A.1 Introdução

A assinatura digital é o mecanismo utilizado para garantir a autoria em documentos eletrônicos. Este processo faz a associação da identidade do signatário a um certificado digital.

Conforme visto em capítulos anteriores, um certificado contém diversos campos. As informações destes campos não podem ser visualizadas sem um elemento que realize o tratamento dos dados.

Nesta capítulos é apresentado o sistema de visualização de certificados digitais desenvolvido no Laboratório de Segurança em Computação - LABSEC.

Na seção A.2 são descritas as janelas do visualizador e suas funcionalidades. Uma breve comparação com outros visualizadores é feita na seção A.3. A seção A.4 trata das considerações feitas sobre o visualizador.

A.2 Apresentação

O Visualizador de certificados digitais foi implementado na Linguagem

C++ utilizando a ferramenta Borland Builder 5.0. Como a proposta inicial era de se implementar um visualizador de certificados digitais, foi utilizado um código fonte público desenvolvido por Peter Guttman, e que faz a decodificação de BER para ASN.1. Essa escolha foi baseada em indicações e variadas referências encontradas sobre a boa qualidade do código desenvolvido por ele. Esse código foi então encapsulado no visualizador de modo a facilitar a implementação do mesmo, eliminando a necessidade de desenvolvimento de um novo decodificador BER.

Executando o visualizador, temos, na janela principal um menubar com as opções "sair", "adicionar registro"e "abrir certificado". Temos também dois botões no canto inferior esquerdo com as mesmas opções para sair e abrir certificado, funcionando apenas como um atalho para facilitar a utilização por parte do usuário. Com maior destaque, encontra-se no centro da tela, "um componente com duas abas". A primeira aba contém uma tela capaz de mostrar uma estrutura em árvore e a segunda um texto. A figura A.1 mostra a janela principal do visualizador.

Quando selecionamos a opção "abrir certificado", temos uma dialog que nos permite escolher arquivos do tipo ".cer". Quando o certificado é aberto, todo o seu conteúdo é mostrado tanto no modo de estrutura em árvore quanto no modo de texto. A estrutura em árvore nos mostra itens relativos ao certificado digital aberto, sem deixar de fora nenhum item relevante. Pode-se ver na A.2 a estrutura de um certificado sendo visualizada.

Sua estrutura, inicialmente, aparece completamente expandida, com os valores de cada campo da estrutura do certificado à mostra. Já na janela de modo texto, A.3 o certificado é apresentado na sua totalidade, com informações e estruturas próprias da linguagem ASN.1. Este texto não pode ser modificado, pois assim o certificado perderia sua validade, e mesmo que assim não o fosse, esta não era a intenção desejada para este software.

A opção "adicionar registro"nos apresenta uma pequena tela contendo campos para que possamos adicionar registros de identificadores de objetos ASN.1 que podem vir a ser encontrados em certificados digitais. Nesta janela dois campos são obrigatórios: "Identificador de Objeto"e "Descrição". Os campos "Comentário"e "Aviso"são

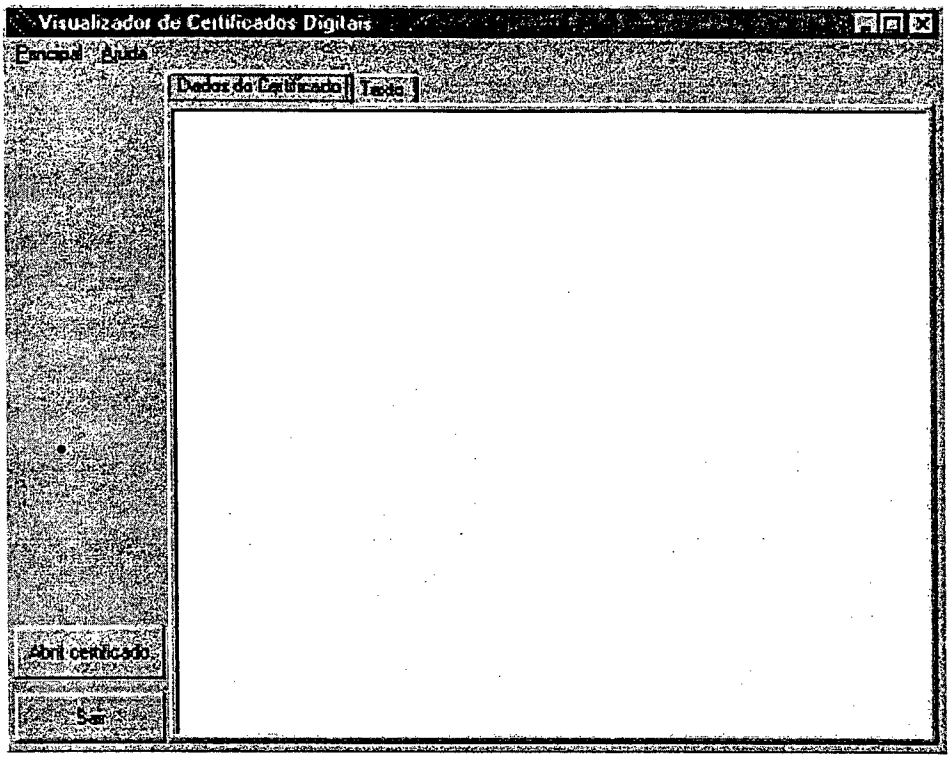

Figura A.1: A janela principal

opcionais. Caso o registro seja inserido, o mesmo será gravado no arquivo "dumpasn1.cfg", que deve estar presente no mesmo local do visualizador. A janela para adição de identificadores de tipos ASN.1 pode ser vista na A.4

Àqueles que desejam saber um pouco mais sobre o visualizador temos uma pequena tela com poucas informações e que pode ser acessada via opção "sobre"no menubar da janela principal. As informações contidas nesta janela são basicamente, período de desenvolvimento, orientador do projeto e uma menção ao código fonte utilizado na decodificação de BER para ASN.1.

A.3 Uma Breve Comparação

Uma Breve comparação com outros visualizadores foi feita para se ter uma idéia de das opções existentes e verificar a as vantagens e desvantagens de cada

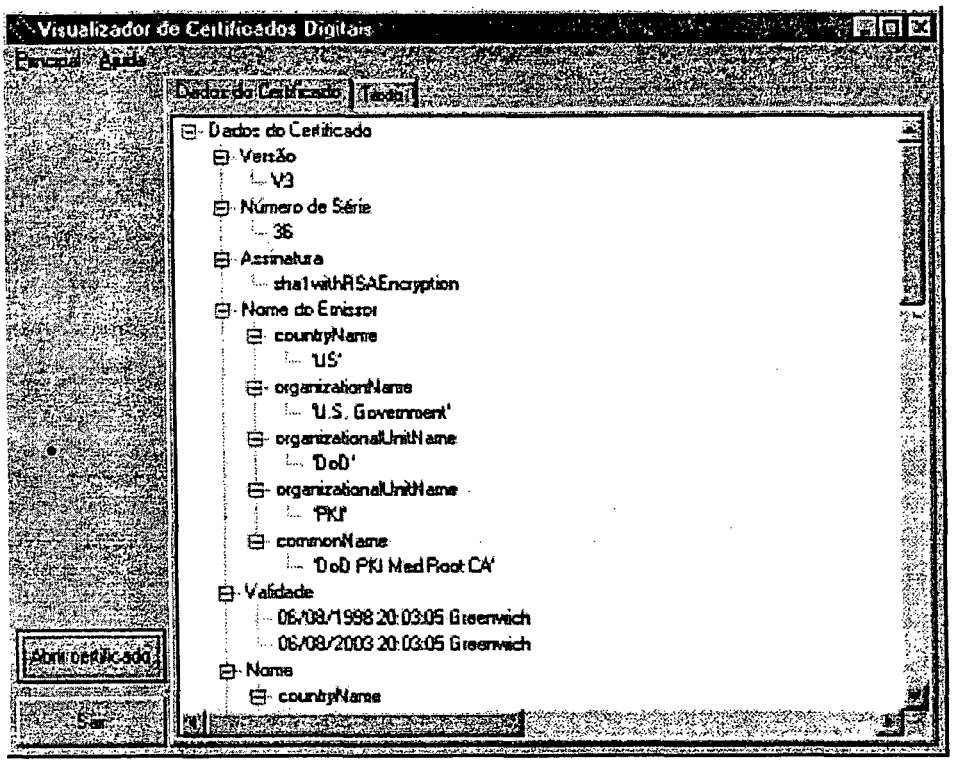

Figura A.2: Visualizando a estrutura interna de um certificado

um. Os visualizadores utilizados na comparação foram:

- O visualizador desenvolvido neste trabalho;
- O visualizador presente no navegador "Internet Explorer"©, que será chamado de visualizador IE;
- O visualizador presente no navegador "Opera"©, que será chamado de visualizador Opera;

Medir as vantagens e desvantagens de cada visualizador se mostrou uma tarefa um tanto subjetiva, por isso nenhuma conclusão foi tirada sobre esta comparação. Serve apenas como ponto de partida para que o leitor faça o seu próprio julgamento.

Os visualizadores dos navegadores possuem uma característica que pode ser uma importante vantagem. O fato de estarem acoplados em um navegador lhes torna

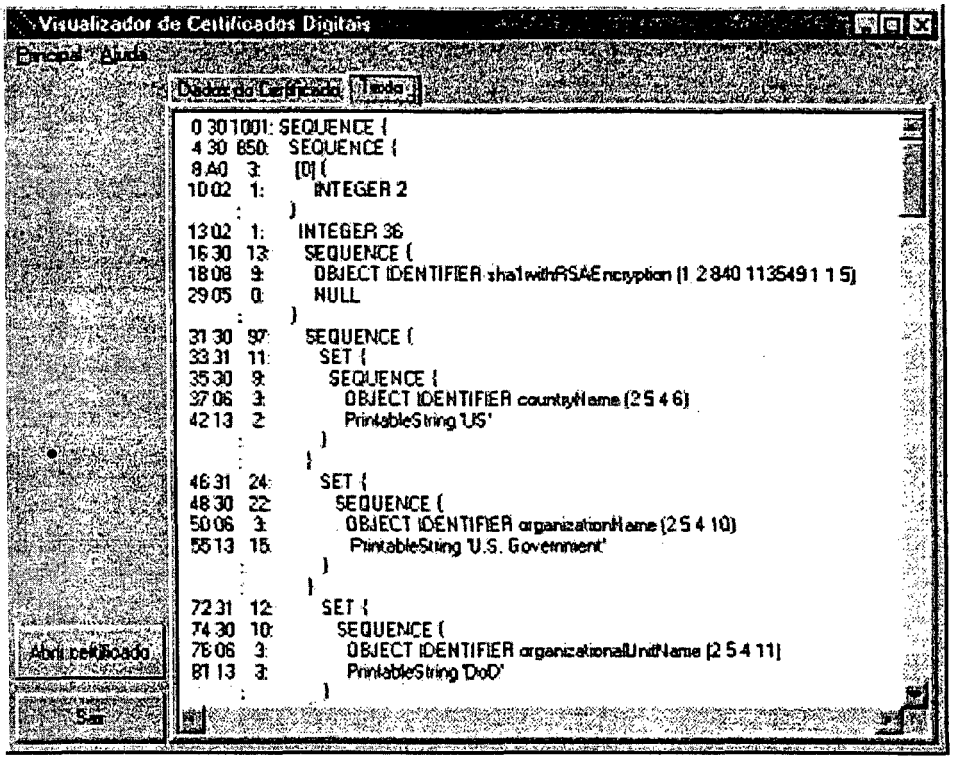

Figura A.3: Visualizando um certificado no modo texto

muito útil quando um usuário está pesquisando páginas na internet e uma das páginas acessadas envia um certificado. Nesse caso, o certificado é automaticamente aberto e mostrado ao usuário. Ele então, pode aceitar, e até instalar o certificado. Certificados instalados recebem confiança permanente do usuário durante sua validade e enquanto permanecerem instalados. No entanto, isso pode ser um empecilho em relação ao visualizador Opera, pois para que o usuário possa visualizar o certificado deve abrir o navegador e então abrir o certificado dentro dele.

A.3.1 Visualizador IE

A interface do visualizador IE não permite que se visualize toda a estrutura de um certificado com acontece com os outros dois visualizadores. Todas as informações aparecem separadas, porém podemos escolher quais campos visualizar, com

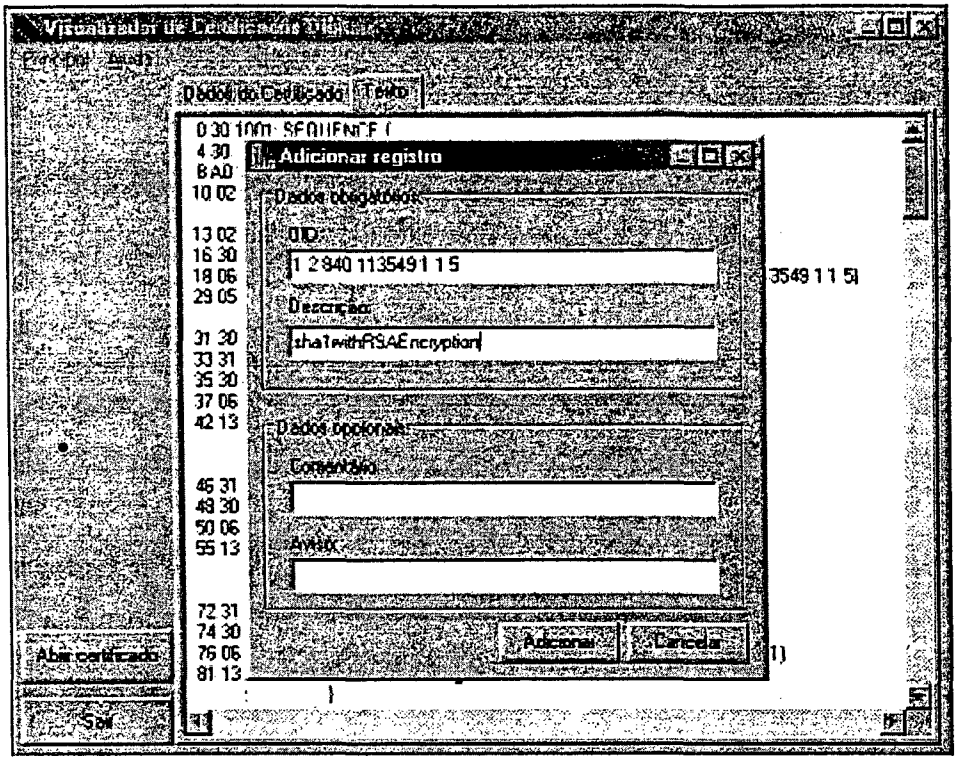

Figura A.4: Adição de identificadores de tipos ASN.1

opções como, "Apenas campos da versão V1".

Algumas informações são omitidas, entre elas os parâmetros da chave pública contida no certificado. Outras parecem não estar corretas, confusas. Isso pode se dar devido ao fato de que o navegador IE analisado era versão língua portuguesa, e podem haver ocorrido perdas de significância de algumas informações durante a tradução do navegador.

A.3.2 Visualizador Opera

O visualizador Opera parece ter qualidade superior ao do navegador IE, com interface mais amigável, mostrando todo o certificado em uma única janela, com informações sobre emissor e dono do certificado em destaque. A quantidade de informações apresentadas é maior e estas são mais detalhadas do que no visualizador IE.

No entanto, depois de alguns certificados, pôde-se constatar que este visualizador também não apresenta todas as informações contidas em alguns certificados digitais, e até mesmo que ele não era capaz de fazer a leitura completa deles, como se algum erro tivesse sido encontrado durante a leitura.

A.3.3 O Visualizador Desenvolvido

Apesar de não estar acoplado diretamente a um navegador, podemos salientar algumas de suas vantagens. Além de mostrar toda a estrutura de um certificado em uma única janela, esse visualizador permite que o usuário ceja o certificado em modo texto tal como ele é escrito na sintaxe ASN.1. Isso permite comparar as informações presentes na estrutura mostrada com as que realmente estão no certificado. A leitura do texto em ASN.1 requer, no entanto, um conhecimento intermediário da estrutura de um certificado. As informações apresentadas ao usuário no modo de estrutura em árvore não necessitam de muito conhecimento para serem compreendidas, pois cada informação recebe um título que dá uma idéia de seu significado. A idealização deste sistema prevê que todas as informações do certificado estejam presentes e detalhadas na estrutura em árvore. Atualmente não há registro de bugs, nem de informações que não estejam aparecendo na estrutura em árvore. Por último, pode-se dizer que o visualizdor implementado durante este trabalho tem uma grande vantagem sobre os outros por se tratar de um sistema com código fonte aberto.

A.4 Considerações

A intenção deste capítulo era de servir como uma prévia do visualizador de certificados digitais, comentar um pouco da sua funcionalidade, para que o usuário tenha uma idéia inicial do que irá encontrar se desejar fazer uso do mesmo. Ainda pode ser útil como um pequeno manual, mesmo que sua utilização seja de extrema facilidade, eliminando qualquer complicação para o usuário.

Este sistema foi desenvolvido visando oferecer à ICP-Brasil uma opção

de visualizador de certificados digitais com código fonte aberto, o que permite que usuários possa ter conhecimento sobre seu processamento. Análises e auditorias podem ser facilmente feitas para verificar se as informações apresentadas no visualizador conferem com as presentes no certificado digital visualizado. Isso dá maior segurança ao usuário, uma vez que, com visualizadores com código proprietário, não podemos saber se há manipulação das informações dos certificados, nem se a leitura de um certificado é feita da maneira correta. Possíveis problemas que possam surgir, apesar da intensa bateria de testes, são rapidamente solucionados.

Aplicativos com código aberto devem ser usados principalmente, na área de segurança. Projetos nessa área não deveriam depender de poucas empresas e tecnologias desconhecidas, nem de sistemas cuja funcionalidade não é realmente conhecida e que não são passíveis de uma análise profunda.