Universidade Federal de Santa Catarina

Programa de Pós-graduação em

Engenharia de Produção

UM MODELO COMPUTACIONAL PARA O FUNCIONAMENTO DA ASSINATURA DIGITAL NO SISTEMA DE INFORMATIZAÇÃO PROCESSUAL

Dissertação de Mestrado

Eliana Cláudia Mayumi Ishikawa

Florianópolis

2003

Universidade Federal de Santa Catarina

Programa de Pós-graduação em

Engenharia de Produção

UM MODELO COMPUTACIONAL PARA O FUNCIONAMENTO DA ASSINATURA DIGITAL NO SISTEMA DE INFORMATIZAÇÃO PROCESSUAL

Eliana Cláudia Mayumi Ishikawa

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de Santa Catarina como requisito parcial para obtenção do título de Mestre em Engenharia de Produção

Florianópolis

2003

Eliana Cláudia Mayumi Ishikawa

UM MODELO COMPUTACIONAL PARA O FUNCIONAMENTO DA ASSINATURA DIGITAL NO SISTEMA DE INFORMATIZAÇÃO PROCESSUAL

Esta dissertação foi julgada e aprovada para a obtenção do título de **Mestre em Engenharia de Produção** no **Programa de Pós-Graduação em Engenharia de Produção** da Universidade Federal de Santa Catarina

Florianópolis, 26 de junho de 2003

_____

Prof. Edson Pacheco Paladini, Dr.
Coordenador do Curso

BANCA EXAMINADORA

_____

Prof. Milton Luiz Horn Vieira, Dr.
Orientador de Orientação

_____ _____

Prof. Alejandro Martins Rodrigues, Dr. Prof. Rogério Cid Bastos, Dr.

Agradecimentos

Agradeço primeiramente a Deus por tudo que fui, que sou e ainda serei e, principalmente por nunca ter me deixado nos momentos mais difíceis.

Ao meu pai Luiz, que mesmo ausente deixou comigo seus princípios e a saudade, a minha mãe Alice pela dedicação e carinho, aos meus irmãos que sempre acreditaram no meu potencial e nunca me deixaram desistir dos meus ideais.

Ao Góis, que nos momentos de maior dificuldade esteve sempre presente e que da sua maneira, vem me incentivando a alcançar os meus objetivos.

Ao professor Leandro Batista de Almeida que dispensou muito do seu tempo e paciência para me esclarecer com seus muitos conhecimentos

A Vanessa Barros, Rosane Martins,Vânia Assis, Ana Paula Perffeto e Gisele Scalabrim , que durante a realização deste trabalho e das longas viagens, tornaram-se pessoas muito especiais.

Ao professor Dr. Milton Luiz Horn Vieira pela sua atenção, compreensão e experiência transmitida no decorrer desses dois anos,

que foram muito importantes para a realização deste trabalho.

A todos que direta ou indiretamente contribuíram para a realização de mais esta conquista, dedico aqui todo o meu agradecimento e carinho.

“Não me entrego sem luta.
Tenho ainda coração.
Não aprendi a me render: que caia o inimigo então.
Tudo passa, tudo passará...
E nossa estória não está pelo avesso assim, sem final feliz.
Teremos coisas bonitas para contar.
E até lá, vamos viver. Temos muito ainda por fazer.
Não olhe para trás – Apenas começamos.
O mundo começa agora – Apenas começamos.”

Metal Contra as Nuvens – Renato Russo

SUMÁRIO

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE REDUÇÕES

Nomes e Siglas

ABA -	American Bar Association
AC Raiz -	Autoridade Certificadora Raiz
AES -	Padrão de Criptografia Avançada - Advanced Encryption Standard
AGP -	Autoridade de Gerência de Políticas
ANSI -	National Institute of Standards in Technology
API -	Apllication Programming Interface
CA -	Certificate Authority - Autoridade Certificadora
CRLs	Certification Revocation Lists - Lista de Revogação de Certificados
DES -	Digital Encryption Standard - Padrão de Criptografia Digital
DH -	Diffie, Hellman
DSA -	Digital Signature Algorithm
DSG -	Digital Signature Guidelines
DSS -	Digital Signature Scheme
EDI -	Eletronic Data Interchange
E-SIGN	Eletronic Signatures in Global And National Commerce - Assinaturas Eletrônicas no Comércio Nacional e Global
FIPS -	Federal Information Processing Standard
HMAC -	Hashed Message Authentication Code - Códigos de Autenticação de Mensagem
IBM -	Information Business Machine
ICP -	Infra-Estrutura de Chave Pública
ICP-Gov -	Infra-Estrutura de Chaves Públicas do Poder Executivo Federal
ICP-OAB	Infra-Estrutura de Chaves Públicas da Ordem dos Advogados
IDEA -	International Data Encryption Algorithm - Algoritmo de Criptografia de Dados Internacionais
IETF -	Internet Engineering Task Force
IPSec -	Internet Protocol Security
ISSO -	International Organization for Standardization
JCA -	Java Cryptography Architecture – Arquitetura de Criptografia Java
JCE -	Java Cryptography Extension – Extensão da Criptografia Java
JDK -	Java Development Kit

JSDK	Java Software Development Kit
JVM -	Java Virtual Machine – Máquina Virtual Java
LCR -	Lista de Certificados Revogados
LDAP -	Lightweight Directory Access Protocol
M.I.T -	Massachussets Institute of Technology
MAC	Código de Autenticação de Mensagem
MD -	Message Digest
Message Digest -	Resumo de mensagem
NIST -	National Institute of Standards and Technology
NSA -	National Security Agency -
OAB-SP -	Ordem dos Advogados do Brasil – São Paulo
OSI -	Open System Interconnection
PGP -	Pretty Good Privacy
PKC -	Public Key Cryptografic
PKI -	Public Key Infrastructure - Infra Estrutura da Chave pública
PRNG -	Pseudo-Randon Number Generators – Gerador de Números Pseudo-Aleatórios
RA -	Registration Authorities - Autoridades de Registro
RC	Ron's Cipher
RSA -	Rivest-Shamir-Adleman
S/MIME -	Secure Multipurpose Internet Mail Extensions
SHA -	Secure Hash Algorithm
SPB -	Sistema de Pagamentos Brasileiros
TRT -	Tribunal Regional do Trabalho
Triple DES -	Triple Digital Encryption Standard – Padrão de Encriptação Digital Tripla
TSA -	Time Stamping Authority - Autoridade Registradora de data/hora
UNCITRAL -	United Nations Commission on International Trade Law
UNCITRAL -	United Nations Commission on International Trade Laic - Comissão das Nações Unidas sobre o Direito do Comércio Internacional
Usenet -	Unix User Network
X.509	Certificado de chave pública criado pela International Telecommunications Union

RESUMO

ISHIKAWA, Eliana Cláudia Mayumi. **Um modelo computacional para o funcionamento da assinatura digital no Sistema de Informatização Processual.** 2003. 129 f. Dissertação (Mestrado em Engenharia de Produção) – Programa de Pós-Graduação em Engenharia de Produção, UFSC, Florianópolis.

A assinatura digital surgiu da necessidade de se garantir a confiabilidade e autenticidade de informações em ambientes computacionais moldados nas tecnologias atuais. O conceito de assinatura digital é aplicado para documentos digitais da mesma forma que o conceito de assinatura comum é usado para documentos impressos que autentica a origem dos dados contidos no mesmo.

O objetivo desta dissertação é apresentar um modelo que possibilite a integração da técnica da assinatura digital no Sistema de Informatização Processual (SIP), desenvolvido pelo Tribunal Regional do Trabalho 14ª Região Rondônia/Acre em parceria com o Departamento de Expressão Gráfica da Universidade Federal de Santa Catarina. Com a integração do modelo proposto, pretende-se aperfeiçoar a segurança do sistema atual e garantir a integridade e a autenticação informatizada de todo e qualquer trâmite processual criado ou alterado pelos usuários do sistema.

PALAVRAS-CHAVES: Criptografia, Algoritmos Criptográficos, Assinatura Digital, Segurança de Dados, Assinatura Digital em Java.

ABSTRACT

The digital signature came out in order to guarantee the reliability and the information authenticity in computing environments according to the current the technologies. The concept of digital signature is applied to digital documents as well as the concept of common signature is used for printed documents which legalize the origin of the information that is on them.

The aim of this dissertation is to present a model that makes possible the integration of the digital signature technique in the Processual Computing System (PCS), development by the 14th Regional Labor Court Rondonia/Acre with a partnership with the Graphic Design Department of Santa Catarina Federal University. It is intended with this model of integration to improve the present system security and guarantee the integrity and the computerized authenticity of any processual procedures created or changed by the system users.

KEY-WORKS: Cryptography, Cryptographic Algorithms, Digital Signature, Data Security, Java Digital Signature.

1 INTRODUÇÃO

A sociedade moderna vive a Era da Informação. Isto se deve às mudanças provocadas pela disseminação e popularização da Internet, que transformou a maneira de se adquirir e, principalmente, de se trocar informações, com um grau de rapidez impossível de ser imaginado anteriormente à nossa época. No entanto, essas transformações tendem a criar um aspecto de impessoalidade nas relações. Como confiar em algo escrito por alguém a milhares de quilômetros de distância? (Volpi, 2001). A solução apontada pelos especialistas em segurança de dados é a implantação da denominada “assinatura digital”.

A assinatura digital será um meio efetivo que garantirá as propriedades de integridade e autenticação dos dados transmitidos na rede ou armazenados em meio computacionais. O processo de implementação de uma assinatura digital é garantido por meio de tecnologias baseadas em um sistema criptográfico assimétrico, composto de um algoritmo ou uma série de algoritmos que irão gerar um par de chaves, sendo uma privada – usada para assinar um documento – e uma chave pública – usada para verificar a validade da assinatura (Schneier, 2001).

Atualmente, a Criptografia apresenta-se como uma ferramenta de grande utilidade para uma série de aplicações, que podem ter diferentes níveis de complexidade (Veloso, 2002). Embora este trabalho descreva, de forma resumida, a matemática subjacente à criptografia, seu foco principal está na utilização dessa tecnologia na aplicação prática de implementar a técnica da assinatura digital em um sistema de computação.

Assim, a proposta do presente trabalho é apresentar um modelo que possibilite a integração da técnica da assinatura digital ao Sistema de Informatização Processual (SIP), desenvolvido pelo Tribunal Regional do Trabalho 14ª Região Rondônia/Acre em parceria com o Departamento de Expressão Gráfica da Universidade Federal de Santa Catarina. Com essa integração, pretende-se aperfeiçoar a segurança do sistema atualmente em uso e garantir a integridade e a autenticação informatizada de todo e qualquer trâmite processual criado ou alterado pelos usuários.

1.1 Origem do Trabalho

A origem deste trabalho encontra-se na parceria estabelecida entre o Departamento de Expressão Gráfica e o Tribunal Regional do Trabalho no desenvolvimento do aplicativo denominado Sistema de Informatização Processual (SIP), e reside na possibilidade de aperfeiçoar a segurança do sistema, integrando ao Módulo de Segurança as tecnologias da assinatura digital e as facilidades inerentes a ela.

Esta integração possibilitará que os usuários possam assinar digitalmente todos e quaisquer trâmites processuais antes dos mesmos serem armazenados no banco de dados e posteriormente, realizar a verificação de validade da assinatura inserida.

1.2 Objetivos

1.2.1 Objetivo Geral

O objetivo geral desta dissertação é especificar um modelo computacional para o funcionamento da assinatura digital no Sistema de Informatização Processual (SIP). Esse modelo surge a partir do acompanhamento e da análise das tecnologias que envolvem a assinatura digital, que incluem as técnicas de criptografia e a descrição de uma modelagem de implementação da assinatura utilizando a Linguagem de Programação Java.

1.2.2 Objetivo Específico

- Realizar uma Revisão Bibliográfica sobre os conceitos relevantes ao projeto, com vistas a formar um suporte teórico sobre o funcionamento da assinatura digital.
- Identificar as principais características e facilidades que a Linguagem de Programação Java oferece na implementação de um processo de assinatura digital.

- Apresentar o Sistema de Informatização Processual (SIP), levando-se em consideração os aspectos de modelagem e funcionalidade.
- Verificar a viabilidade de integração da assinatura digital ao Módulo de Segurança do sistema.
- Explicar de que forma os recursos de assinatura digital serão utilizados no SIP.

1.3 Procedimentos Metodológicos

Primeiramente, realizou-se uma pesquisa que utilizou recursos bibliográficos diversos, tais como livros e pesquisas na Internet (artigos, tutoriais), com o objetivo de apresentar o atual estado da arte relaciona à assinatura digital, em que foram priorizados os aspectos técnicos, práticos e legais.

Pela constatação de que a assinatura digital está embasada na adoção da criptografia assimétrica, esta foi privilegiada na pesquisa quanto a seus aspectos técnicos, com a apresentação dos algoritmos mais utilizados para gerar chaves criptográficas em assinaturas e certificados digitais.

Ao lado dos problemas técnicos, constatou-se que os aspectos práticos e legais referentes ao tema também seriam relevantes à pesquisa e, por isto, foram trabalhadas algumas questões a eles relacionados, tais como: onde a assinatura digital pode ser empregada? quais são as abordagens legislativas sobre o tema no Brasil? e no exterior?.

Especificamente quanto ao objetivo de propor um modelo utilizando a técnica da assinatura digital em um determinado sistema computacional, foi necessário efetivar um levantamento para identificar as funcionalidades do aplicativo denominado Sistema de Informatização Processual (SIP). Para cumprir essa etapa, foram necessárias várias reuniões com os técnicos responsáveis pelo desenvolvimento do SIP, nas quais foram analisados os seguintes tópicos:

- A disponibilidade de recursos físicos e monetários.
- A viabilidade de integração da técnica de assinatura digital no Módulo de Segurança.
- A definição de quais módulos necessitariam da assinatura digital.
- O levantamento do ambiente de aplicação.

- A definição de como deveria ser a interface desses módulos com o usuário.

Ao se definir o ambiente de aplicação, desenvolveu-se um estudo sobre as principais características da Linguagem de Programação Java e das ferramentas disponíveis para se criar uma assinatura digital, assim como buscou-se a definição de quais os algoritmos seriam utilizados em todo o processo de assinatura. A partir do resultado deste estudo, foi proposto um modelo para se gerar chaves, assinar e verificar uma assinatura de arquivos.

Por fim, foi apresentado um o modelo que possibilitaria a integração da técnica da assinatura digital no aperfeiçoamento da segurança do Sistema de Informatização Processual.

1.4 Descrição e Organização dos Capítulos

Este trabalho está estruturado em cinco capítulos distribuídos da seguinte forma:

1. Capítulo 1 – A presente Introdução, onde estão apresentados os seguintes itens: origem do trabalho, os objetivos e os procedimentos metodológicos.

2. Capítulo 2 – Neste capítulo é apresentada a revisão da literatura sobre o assunto, constituindo-se como fundamentação teórica para a criação de um processo de assinatura digital. Nele são apresentados os conceitos básicos sobre Criptografia, os principais algoritmos criptográficos, conceitos e técnicas aplicadas a uma assinatura digital e a certificados digitais, além de um breve histórico sobre as abordagens legislativas relativas ao tema.

3. Capítulo 3 – Trata das principais características e das facilidades que a Linguagem Java oferece para se implementar um processo de assinatura digital. Este capítulo descreve, também, uma proposta de modelagem utilizando as facilidades da linguagem em todas as etapas de criação de uma assinatura digital: geração de chaves de assinatura, geração da assinatura e a verificação.

4. Capítulo 4 – Neste capítulo se procede à descrição do Sistema de Informatização Processual (SIP), seus principais objetivos, características e

funcionalidades de cada módulo e efetiva-se a apresentação do modelo proposto para a utilização das tecnologias da assinatura digital no SIP.

5. Capítulo 5 – Apresenta uma análise de todo o trabalho realizado, compreendendo as justificativas e conclusões do modelo proposto, bem como as contribuições e recomendações deste trabalho para futuros estudos.

2 REVISÃO DA LITERATURA

2.1 Criptografia

A criptografia existe há milhares de anos. Há evidências de que ela já se encontrava presente no sistema de escrita hieroglífica dos egípcios e em documentos de generais gregos e romanos. Desde então, a criptografia tem sido muito utilizada, principalmente para fins militares e diplomáticos.

Formada a partir da concatenação dos termos gregos *kryptos* (escondido, oculto) e *graphé* (grafia, escrita), a Criptografia constituiu-se como a ciência de escrever em códigos ou em cifras, ou seja, uma ciência capaz de prover meios pelos quais se torna possível transformar um texto “claro” (legível) em um texto “cifrado” (ilegível) (Panetta, 2000).

No âmbito da computação, a criptologia constitui-se em importante instrumento para que se possa garantir a segurança em todo e qualquer ambiente computacional que demande sigilo em relação às informações e dados com os quais trabalha. Ela pode, por exemplo, ser usada para codificar dados e mensagens – antes de serem enviados por vias de comunicação – que, ainda que sejam interceptados, dificilmente seriam passíveis de decodificação por possíveis interceptadores. Para tanto, são utilizadas funções matemáticas e uma senha especial chamada “chave”.

Para Terada (2000, p.16), a Criptografia pode ser descrita como:

> “a ciência que estuda a transformação de dados de maneira a torná-los incompreensíveis sem o conhecimento apropriado para a sua tradução, tornando os conteúdos secretos, evitando riscos internos e externos que venham a ocorrer durante o trajeto dos dados enviados, que são convertidos em um código que só poderão ser traduzidos por quem possuir a “chave” secreta, enquanto que a Criptoanálise executa o processo inverso, sendo a ciência que estuda a decifração, tornando o código compreensível.”

A figura 1, mostra esquematicamente, como se dá o processo criptográfico na transmissão de dados e/ou informações.

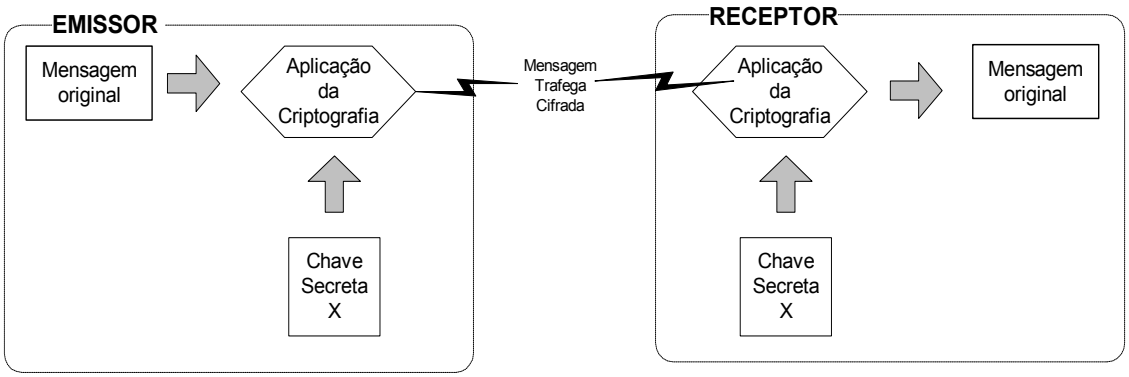

FIGURA 1.Ilustração de um processo simples de criptografia no envio da mensagem.

Fonte: Volpi (2000, p.7).

Segundo Garfinkel & Spafford (1999, p.209) as quatro palavras chave usadas para descrever todas as diferentes funções que a criptografia desempenha nos sistemas modernos de informação são:

- **Confidencialidade ou Privacidade:** utilizada para embaralhar as informações enviadas por teletransmissão (geralmente pela Internet) e armazenadas em um servidor, de forma que os invasores não possam acessar o conteúdo dos dados. Refere-se à proteção de informações privadas (confidenciais ou não) contra o uso ou agregação impróprios. Impede que pessoas não autorizadas tenham acesso ao conteúdo da mensagem ou parte dela, e que, posteriormente, essas pessoas possam utilizar os dados obtidos de forma desautorizada para interferir sobre o todo. Sua finalidade é garantir que apenas a origem e o destino tenham conhecimento do exato teor das informações;

- **Autenticação:** garante a identidade de quem está enviando a mensagem. O receptor da mensagem pode verificar a identidade da pessoa que a assinou. Pode ser implementada a partir de um mecanismo de senhas ou de assinatura digital;

- **Integridade:** cuida para que o conteúdo da mensagem não seja modificado em trânsito. Os dados recebem um tratamento que os transformam em caracteres

não legíveis, garantindo que qualquer receptor, que não o destinatário dos dados, fique impedido de modificá-los ou deles se apropriar. Dessa forma, a informação transmitida em um ponto é a mesma recebida em outro.

- **Não – repúdio:** tem a função de fazer com que o autor de uma mensagem não possa negar falsamente que a tenha enviado. Assim, se uma entidade enviou uma mensagem a outra entidade, não podem negar a autoria ou o recebimento. Usa-se, para tanto, procedimentos criptográficos, aliados a técnicas de assinatura digital.

2.1.1 Chaves

Conforme descrito anteriormente, o papel da criptografia na segurança de dados é basicamente converter informações sigilosas em algo sem sentido, sendo necessário encriptar (codificar, criptografar, cifrar) os dados na emissão, e, assim que esses dados cheguem a seu destino, convertê-los de volta à forma de informação, decriptando-os (decodificando, descriptografando, decifrando); para isto, utiliza-se um algoritmo.

A palavra “algoritmo” é um termo utilizado para nomear uma “receita” de procedimentos, passo a passo . Pode-se dizer que um algoritmo é uma lista de instruções, que deverão ser executadas em uma determinada ordem, ou, ainda, que é uma lista rígida de comandos a ser seguida; essa lista pode conter uma série de perguntas e, dependendo das respostas, descreve os passos apropriados a serem seguidos. (Burnett & Paine,2002)

A implementação de um algoritmo em um programa de computador significa que o programa converte a lista de comandos, perguntas e operações do algoritmo em uma linguagem de computador, permitindo que o mesmo realize os passos em uma ordem apropriada.

Na criptografia computadorizada, os algoritmos são, às vezes, operações matemáticas complexas e, outras vezes, apenas manipulações de bits. Existem vários algoritmos de criptografia e cada um tem sua própria lista de comandos ou passos. É possível haver um programa que implemente um algoritmo de criptografia

que procede pela conversão dos dados recebidos em algo sem sentido; isso exige, necessariamente, o uso de uma chave. (Terada, 2000).

As chaves são elementos fundamentais que interagem com os algoritmos para a cifragem/decifragem das mensagens. O algoritmo realiza seus passos utilizando a chave para alterar o texto normal e convertê-lo em texto cifrado. Para desbloquear o arquivo encriptado, é necessário inserir a mesma chave para executá-lo. O algoritmo inverte os passos e converte o texto cifrado de volta ao texto normal original, como ilustrado na figura 2, abaixo:

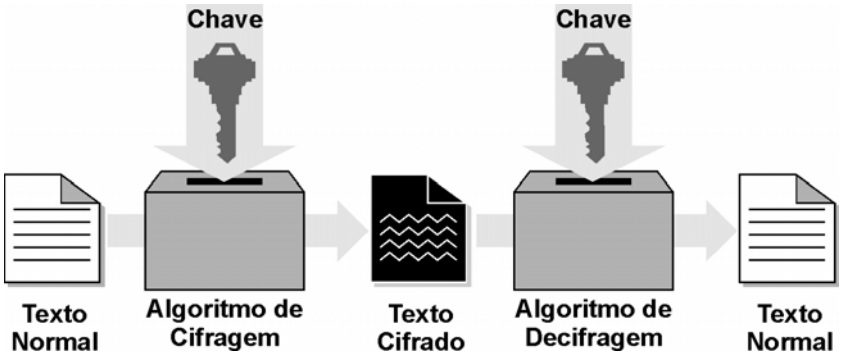

FIGURA 2 - Ilustração de um processo de cifragem e decifragem com chaves.

Fonte: GARFINKEL, Simson; SPAFFORD, Gene (1999, p.189).

As chaves de criptografia são similares às senhas de acesso a bancos e a sistema de acesso a computadores; a utilização da senha correta torna possível ter acesso aos serviços, em caso contrário, o acesso é negado. No caso da criptografia, o uso de chaves relaciona-se com o acesso ou não à informação cifrada. O usuário deve usar a chave correta para poder decifrar as mensagens.

Assim como as senhas, as chaves na criptografia também possuem diferentes tamanhos, pois seu grau de segurança está relacionado à sua extensão, ou seja, quanto maior for a senha de um usuário, maior será o grau de confidencialidade da mensagem. Na criptografia, as chaves são longas seqüências de bits, assim uma chave de três dígitos oferecerá oito ($2^3 = 8$) possíveis valores para a chave (Lynch & Lundquist,1996).

Toda criptografia computadorizada não opera somente com o algoritmo, mas sim em conjunto com a chave, pelo simples fato de que, se o interceptador conhecer o algoritmo, torna-se possível recuperar os dados secretos simplesmente executando o mesmo. (Oaks, 1999). Dessa forma, as chaves aliviam a necessidade de se preocupar em proteger o algoritmo utilizado no esquema de criptografia.

Há basicamente dois tipos de criptografia em relação ao uso de chaves. Quando é utilizada a mesma chave, tanto para cifrar quanto para decifrar uma mensagem, o método adotado é chamado de sistema de criptografia por chave simétrica ou chave secreta. Caso se utilizem chaves diferentes na cifração e na decifração de uma mensagem, nomeia-se o sistema como sendo de chaves assimétricas ou chave pública.

2.1.2 Criptografia Simétrica ou de Chave Secreta

O princípio básico deste conceito, conhecido também como Criptografia Convencional, é o uso de uma chave secreta, que o emissor utiliza para a codificação da informação, e posteriormente, o destinatário a utiliza para decifração da informação. Nesse sistema, tanto o emissor quanto o receptor da mensagem cifrada devem compartilhar a mesma chave, que, para preservação do sigilo, deve ser mantida em segredo por ambos.

Como citado anteriormente, a Criptografia Simétrica está baseada em uma única chave. A figura 3 ilustra este processo de forma clara, mostrando que a mesma chave que propicia a cifragem da mensagem é utilizada para sua posterior decifragem.

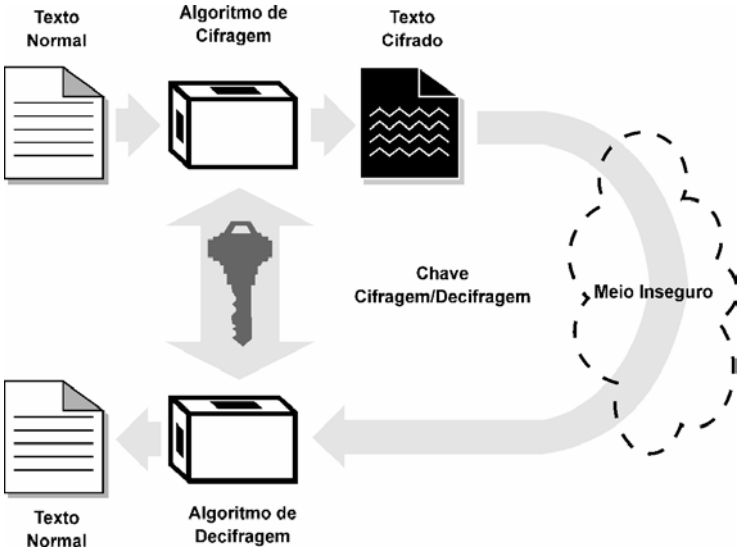

FIGURA 3 -Ilustração de um processo de criptografia por chave secreta

Fonte: GARFINKEL, Simson; SPAFFORD, Gene (1999, p.197).

Levando-se em consideração os princípios da criptografia simétrica, fica evidente a importância do sigilo sobre a chave utilizada para criptografar a mensagem. Assim,

um dos aspectos desfavoráveis desse método é o processo de distribuição de chaves. Segundo Stallings (1999, p.141), o maior problema deste tipo de sistema é garantir que o emissor e o destinatário de uma mensagem cifrada pelo algoritmo – e somente eles – possam conhecer a chave secreta ora em uso. Além disso, existe a necessidade de transmitir a chave secreta por um meio seguro, separadamente da mensagem, e de efetivar combinações prévias sobre futuras alterações da mesma.

Isto requer a existência de um método pelo qual as duas partes possam se comunicar de modo seguro, seja pessoalmente ou através de um sistema de entrega (seja ele o telefone ou outro meio de transmissão confiável) capaz de garantir a segurança do sigilo. Caso esse passo do processo sofresse quebra de sigilo, nessa forma de distribuição de chaves, qualquer interceptador poderia ter acesso tanto à mensagem, quanto a sua chave secreta.

Outro problema que ocorreria nesse processo seria o caso de três pessoas – A, B e C – que queiram se comunicar utilizando chaves secretas. Seriam necessárias 3 (três) chaves: uma compartilhada entre A e B, outra entre A e C, e a última entre B e C, como descrito pela figura abaixo.

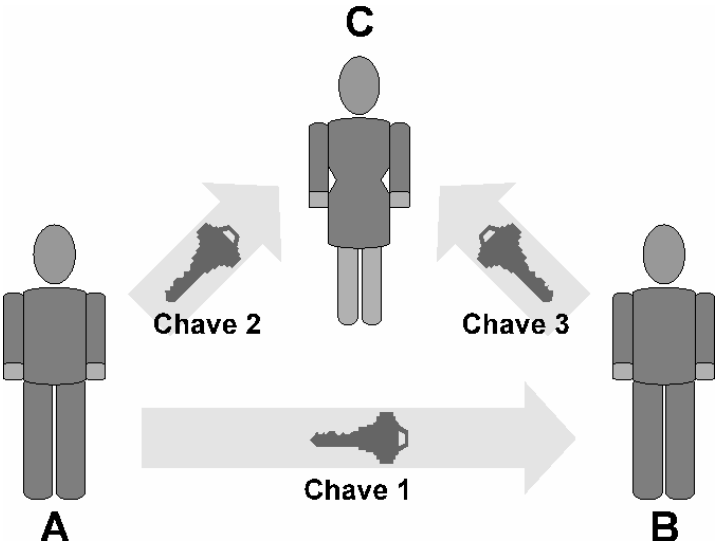

FIGURA 4 -Ilustração de um processo de criptografia por chaves secretas
Fonte: GARFINKEL, Simson; SPAFFORD, Gene (1999, p.199).

Se mais pessoas fossem incluídas neste sistema de comunicação, mais chaves serão necessárias. No caso de mais duas pessoas, mais sete chaves seriam necessárias. Generalizando, quanto mais pessoas quiserem se comunicar utilizando chave secreta simétrica, um número muito grande de chaves seria necessário, pois a função que explicita o número de chaves é exponencial, gerando um grande

problema para o gerenciamento de chaves utilizadas por grandes grupos de usuários.

Por sua vez, nos sistemas modernos de criptografia, as chaves simétricas são bem mais rápidas que os algoritmos de chave pública (relatados a seguir com mais detalhes). Além disso, as chaves simétricas podem ser implementadas mais facilmente. (Garfinkel & Spafford, 1999).

2.1.2.1 Principais Algoritmos Simétricos

A seguir serão descritos os principais algoritmos de chave secreta:

a) Padrão de Criptografia Digital - Data Encryption Standard (DES)

Baseado num algoritmo desenvolvido pela IBM, chamado Lúcifer, seu propósito foi criar um método padrão para proteção de dados.

Foi adotado pelo governo dos Estados Unidos em 1977, e como padrão do ANSI – *American National Standards Institute* (Instituto Nacional Americano de Normas). Este algoritmo é o mais amplamente usado internacionalmente ainda hoje, e foi um avanço científico significativo no sentido de ter se constituído no primeiro algoritmo de criptografia tornado público, pois até então todos os algoritmos do gênero eram secretos. (Terada, 2000).

Fundamentalmente, o DES realiza somente duas operações sobre sua entrada: deslocamento de bits e substituição de bits. A chave controla exatamente como esse processo ocorre. Ao fazer estas operações repetidas vezes e de uma maneira não-linear, chega-se a um resultado que não pode ser revertido à entrada original sem o uso da chave.

O algoritmo possui 64 bits, tanto de entrada como de saída e uma chave de 56 bits para criar uma tabela de chaves. Utilizando a tabela de chaves, o DES realiza manipulações de bits sobre o texto simples e, para decriptar o texto cifrado, simplesmente faz o processo inverso.

Ao longo da década de 1980, o consenso dos criptógrafos era de que o DES não tinha nenhuma fraqueza: utilizando força bruta – pois, para quebrar uma chave de 56 bits, um número entre 0 e 73 quadrilhões, aproximadamente, de combinações

possíveis, seriam necessários vários anos para se decifrar uma única mensagem, mesmo utilizando o computador mais rápido da época – parecia que o DES não deixava margem à quebra de sigilo.

Mas, a partir da década de 1990, os computadores se tornaram mais rápidos e, conseqüentemente, mais ágeis para montar em um curto período o texto cifrado, o que mostrou que o DES não seria assim “tão forte”. Em 1999, na RSA Conference, a Eletronic Frontier Foundation quebrou a chave de DES em menos de 24 horas. (Burnett & Paine, 2002).

Esse algoritmo, atualmente, pode não ser apropriado para confidencialidade de informações de longa duração (por exemplo para informações diplomáticas que devem ser mantidas sobre sigilo por mais de 40 anos), mas pode ser totalmente adequado para proporcionar segurança em informações confidenciais de curta duração (por exemplo, nos dados de uma aplicação de transferência eletrônica de fundos em sistemas bancários fechados) (Albertin, 1999).

b) Triple DES

Um substituto ao DES, amplamente utilizado é o chamado “Triple DES”. Seu diferencial em relação ao DES é a utilização do algoritmo de criptografia por três vezes, com chaves diferentes, tornando-se pelo menos duas vezes mais seguro que o DES original. Primeiramente, executa-se o DES no bloco de dados, utilizando-se uma chave e, então, encripta-se esse resultado com uma outra chave de DES. Em seguida, efetiva-se o mesmo procedimento uma terceira vez, como mostra a figura 5:

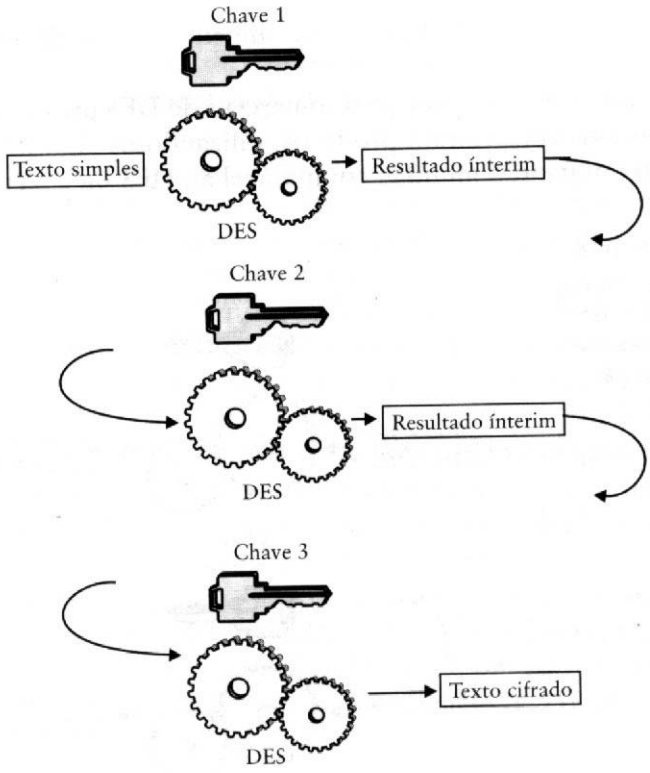

FIGURA 5 - Ilustração de um processo de criptografia utilizando o Triple DES

Fonte: BURNETT, Steve; PAINE, Stephe (2002, p.42).

Cada uma das três chaves possui 56 bits. Essencialmente, seria como utilizar uma chave de 128 bits. No entanto, para quebrar a chave, seriam necessárias muito mais que 24 horas, pois, partindo-se do princípio de que se levaria 24 horas para quebrar cada chave, para saber se a primeira chave foi quebrada, seria necessário combiná-la com as duas outras corretas, uma de cada vez, alongando o tempo de processamento para descoberta das chaves. O texto simples correto que houvesse sido criptografado por esse processo apareceria apenas quando todas as três chaves fossem corretas. (Burnett & Paine, 2002).

Uma das maiores desvantagens desse algoritmo seria o fato de que o DES original já tomava muito tempo para encriptar ou decriptar dados e o Triple DES é três vezes mais lento. Outro problema advém do fato de que os analistas criptográficos descobriram uma maneira de simplificar o ataque de força bruta de formas inteligentes, para reduzir de 168 bits para 108 bits. Apesar de ainda “segura”, essa fraqueza incomoda.

c) Padrão de Criptografia Avançada - Advanced Encryption Standard (AES)

Em Janeiro de 1997, o órgão oficial norte-americano NIST – *National Institute of Standards in Technology* (Instituto Nacional de Normas em Tecnologia) anunciou formalmente um plano para definir um algoritmo como o novo padrão para criptografia. Abriu uma espécie de "concurso" em que qualquer pessoa poderia submeter um algoritmo, com a seguinte condição: o vencedor não teria quaisquer direitos quanto à propriedade intelectual do algoritmo selecionado. Os critérios para avaliação dos algoritmos que viessem a concorrer seriam: segurança, desempenho (rápido em várias plataformas) e tamanho (não poderia ocupar muito espaço nem utilizar muita memória). (Barker. et.al, 2000).

Os algoritmos foram analisados por técnicos da área espalhados pelo mundo e, em 20 de agosto de 1998, foram selecionados 15 algoritmos originais. Mas todos foram eliminados, devido a fraquezas existentes neles ou, simplesmente, porque se revelaram muito grandes ou muito lentos.

Em agosto de 1999, o NIST, novamente, anunciou uma seleção de cinco algoritmos finalistas, que passaram, então, a ser analisados por pesquisadores, analistas de criptografia e fornecedores de hardware e de software do mundo todo. E, finalmente, em 2 de outubro de 2000, o algoritmo escolhido foi o chamado Rijndael, inventado por dois pesquisadores belgas: Vincent Rijmen e Joan Daemen. (Burnett & Paine, 2002).

O Padrão de Criptografia Avançada - AES (Advanced Encryption Standard) especificou, então, o Rijndael como o novo algoritmo de criptografia simétrica. Esse padrão passou a ser usado pelo governo americano para proteger informações restritas.

Segundo Burnett & Paine (2002, p.43), "o algoritmo AES está livremente disponível para qualquer pessoa desenvolver, utilizar ou vender. Como o DES, é esperado que o AES torne-se um padrão mundial."

O AES usa um número variável de tamanho de chave e tamanho de bloco. Atualmente, sua especificação de trabalho é possuir chaves com tamanhos que variam entre 128, 192 e 256 bits, criptografando blocos de 128, 192 e 256 bits (todas as nove combinações de tamanho de chave e tamanho de blocos são possíveis). Além disso, esses números podem ser facilmente expandidos para múltiplos de 32 bits. O AES possui facilidade de implementação, propiciando uso em Smart Cards e

outros equipamentos que utilizam pouca memória RAM; além disso, utiliza poucos ciclos de processamento.

O código desse algoritmo é bem enxuto e não depende de nenhum outro tipo de componente criptográfico, como números randômicos. Esse aspecto faz com que sua utilização apresente um nível de segurança superior. (Stohler, 2002).

d) RC2, RC4 e RC5

Em resposta aos problemas encontrados na utilização do Triple DES, vários criptógrafos desenvolveram novas cifras de bloco. Dentre os mais populares, podem ser citados o RC2, o RC4 e o RC5. Esses algoritmos foram desenvolvidos originalmente por Ronald Rivest, da RSA Data Security.

O RC2 foi revelado por uma mensagem anônima na Usenet em 1994, assim como o RC4 em, 1996 e pareceram ser relativamente poderosos, embora algumas chaves sejam vulneráveis. Ambos são implementações que permitem a utilização de chaves de 1 a 2048 bits, embora, muitas vezes, o tamanho da chave seja limitado a 40 bits no software vendido para exportação.

Com chaves pequenas (menores que 48 bits), tanto o RC2 quanto o RC4 são códigos fáceis de serem quebrados, e não se tem muitas informações sobre sua segurança com chaves extensas. O RC2 é uma cifra de bloco, similar ao DES. O RC4 é uma cifra de corrente, onde o algoritmo produz uma corrente de pseudo-números que são cifrados através de uma operação lógica XOR, junto com a própria mensagem. O RC5 permite que o tamanho da chave , o tamanho de blocos de dados e o número de vezes que a criptografia será realizada sejam definidos pelo usuário. (Garfinkel & Spafford,1999).

e) International Data Encryption Algorithm – IDEA

O IDEA (sigla que designa *International Data Encryption Algorithm* – Algoritmo de Criptografia de Dados Internacionais) é um algoritmo de cifragem de bloco desenvolvido em Zurique, na Suíça, por James L. Massey e Xuenjia Lai, e tornado conhecido, através de publicação, em 1990 (Garfinkel & Spafford, 1999). É um algoritmo que utiliza uma chave de 128 bits e tanto o texto legível (entrada) como o texto ilegível (saída) utilizam 64 bits. Foi projetado para ser eficiente em implementações por software e possui patente nos EUA e na Europa da Ascom-Tecvh AG.

O IDEA possui uma estrutura semelhante ao DES, com um número fixo de iterações de uma mesma função, utilizando subchaves distintas e possuindo o mesmo algoritmo com a finalidade de criptografar e descriptografar, alterando-se, em relação àquele, na forma de geração de subchaves. (Stallings, 1999).

É um algoritmo que ainda não pode ser conceituado como forte, devido a seu pouco tempo de vida, porém aparenta ser robusto. Sua chave, com 128 bits, elimina a possibilidade de alguém usar computadores atualizados mais velozes para efetivar-lhe ataques por força bruta. (Terada, 2000).

2.1.3 Criptografia Assimétrica ou de Chave Pública

Terada (2000, p.95), relata que a criptografia de chave pública foi postulada pela primeira vez em meados da década de 70 por Whitfield Diffie e Martin Hellman. Os dois pesquisadores, na época na universidade de Stanford, investigavam a criptografia em geral e o problema de distribuição de chaves em particular, e escreveram um artigo em que propunham a implementação de um esquema por meio do qual duas pessoas poderiam criar uma chave secreta compartilhada trocando informações públicas, comunicando-se por meio de linhas públicas, utilizando para tanto duas chaves: uma privada e a outra pública.

A técnica relatada pelos pesquisadores, conhecida como chave pública ou criptografia assimétrica, consiste numa mistura de dados ininteligíveis em que a chave privada, mantida em sigilo, é utilizada pelo emissor para cifrar uma mensagem. Já a chave pública deve ser publicada e amplamente divulgada, fazendo com que qualquer pessoa possa utilizá-la para enviar mensagens cifradas, ou seja, tornando-se disponível para todos aqueles que poderão ter acesso ao conteúdo da mensagem.

As duas chaves são relacionadas através de um processo matemático, usando funções unidirecionais para a codificação da informação. (Garfinkel & Spafford, 1999).

A figura 6, demonstra um processo de cifragem de uma mensagem utilizando a chave pública e a decifragem, que só pode ocorrer com o uso de uma chave distinta, a chave secreta, com a qual está relacionada.

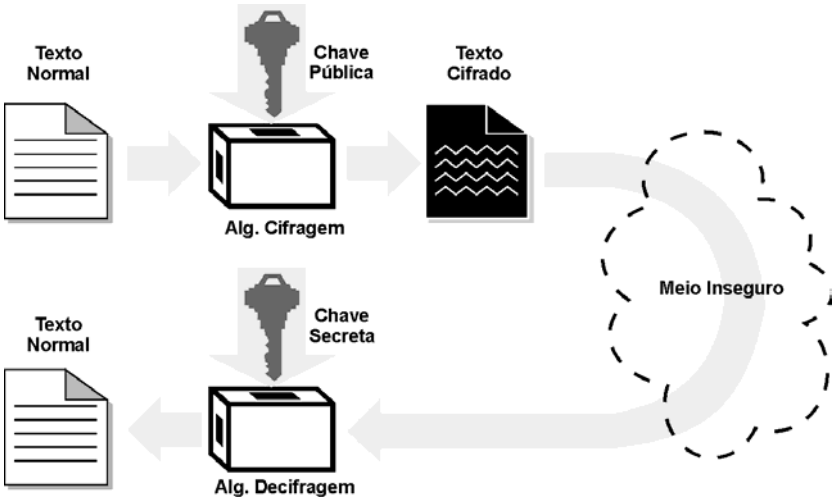

FIGURA 6 - Ilustração de um processo de criptografia por chave pública
Fonte: GARFINKEL,Simsom; SPAFFORD, Stephe (2001, p.208).

Desta maneira, caso o interceptador tenha o conhecimento da chave secreta de cifragem, torna-se impossível a alteração da mesma com o uso dessa chave, pois a chave utilizada para cifrá-la não é a mesma para decifrá-la.

Como citado anteriormente, na criptografia simétrica (chave secreta), utilizando-se uma única chave, existe um procedimento passo a passo para encriptar os dados de saída e, para descriptá-los, basta que se invertam os passos. Desta forma, é possível observar que a utilização deste método torna-se pouco viável, quando se pretende criar uma comunicação segura entre pessoas comuns, se comparada com a utilização da criptografia assimétrica (chave pública).

Os problemas de distribuição de chaves existentes na criptografia por chave secreta são sanados com a utilização da chave pública, pois não há necessidade do compartilhamento de uma mesma chave nem de um pré-acordo entre as partes interessadas. Com isto o nível de segurança é maior. (Schneier, 1996).

A figura 7, demonstra um processo de criptografia utilizando-se chave pública e privada no envio e recebimento da mensagem.

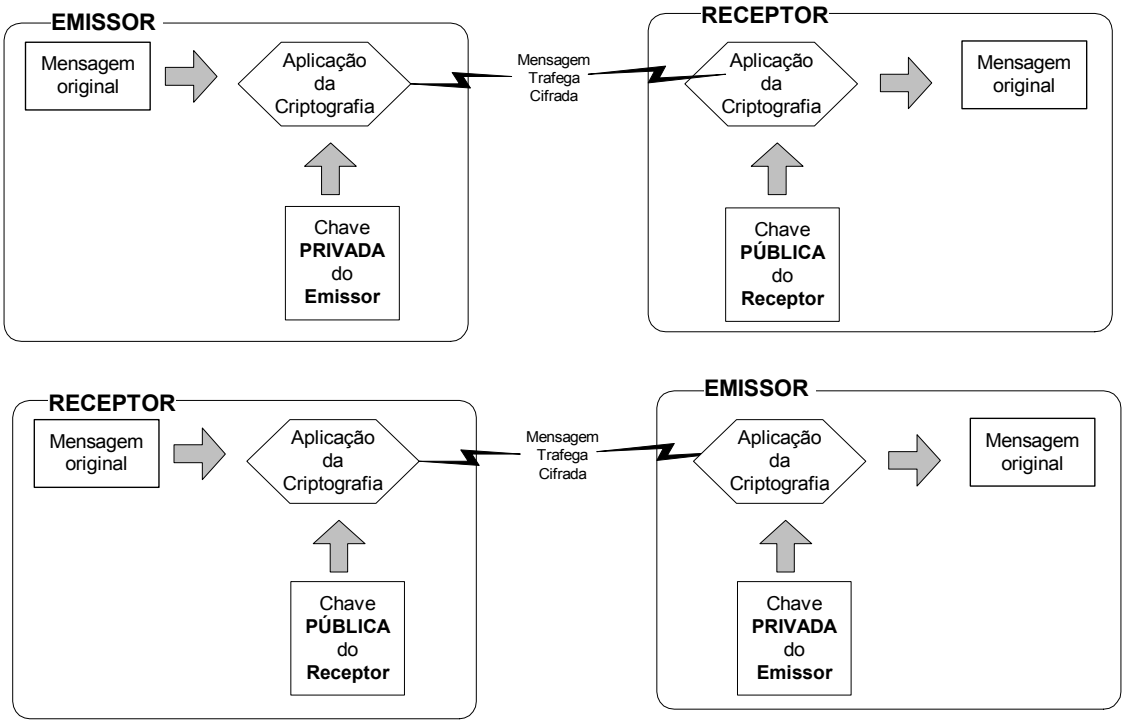

FIGURA 7 - Ilustração de um processo de criptografia por chave pública

Fonte: VOLPI, Marlon M. (2001 p.14)

A mensagem cifrada pelo emissor, utilizando a chave privada, só poderá ser decifrada pelo receptor utilizando a chave pública do mesmo. Caso o receptor venha a enviar uma mensagem cifrada ao emissor, utilizando a chave pública do mesmo, essa mensagem só poderá ser decifrada utilizando-se a chave privada do próprio emissor.

Caso a mensagem enviada pelo emissor e sua respectiva chave pública forem interceptadas, o interceptador não terá condições de criar uma nova mensagem para o receptor, levando em consideração que a codificação através da chave pública somente permite a leitura do possuidor da chave privada, o que não é o caso do receptor. No entanto, o interceptador poderia enviar uma mensagem para o emissor utilizando a chave pública deste, o qual possui a chave privada, o que permite sua leitura. Para que esse processo fosse evitado, seria necessário que tanto o emissor quanto o receptor tivessem, cada um deles, uma chave privada e uma pública.

Desde então, a partir do artigo publicado por Whitfield Diffie e Martin Hellman, vários sistemas de chave pública já foram desenvolvidos. Infelizmente, houve muito

menos desenvolvimento de algoritmos de chave pública em relação aos de chave simétrica. A razão disso está relacionada ao modo como esses algoritmos são criados. (Sawicki,1993). Um bom algoritmo de chave simétrica simplesmente embaralha os dados de entrada e o desenvolvimento de um novo algoritmo de chave simétrica depende da criação de novas maneiras de executar esta operação de forma confiável. Os algoritmos de chave pública são baseados na teoria dos números. O desenvolvimento de novos algoritmos de chave pública requer a identificação de novos problemas matemáticos, cujas particularidades mostrem propriedades matemáticas diferenciadas.

Segundo Garfinkel & Spafford (2001), além do ganho da segurança em relação às chaves secretas, existe uma conveniência adicional na chave pública, uma vez que ela nunca precisa ser repetida ou revelada. Outra vantagem é a sua capacidade de prover assinaturas digitais, para comprovar a origem e a integridade dos dados. No entanto as chaves públicas apresentam um problema significativo: são muito lentas. Na prática, os algoritmos de criptografia e de decifragem da chave pública são entre 10 e 100 vezes mais lentos do que os equivalentes de chave simétrica.

No quadro abaixo (Quadro 1) é ilustrado o resumo de alguns dos aspectos importantes da criptografia convencional (simétrica) e de chave pública (assimétrica).

Quadro 1 – Principais diferenças: Encriptação Convencional e de Chave pública

Encriptação convencional	Encriptação de chave pública
Necessidade para trabalhar:	
O mesmo algoritmo e a mesma chave são usados para a encriptação e descriptação.	Um algoritmo é usado para encriptação e descriptação com um par de chaves: uma para encriptação e a outra para a descriptação.
O emissor e o receptor devem compartilhar o algoritmo e a chave.	O emissor e o receptor devem ter o par de chaves (privada e pública).
Necessidade para a Segurança:	
A chave deve ser mantida em segredo.	Uma das duas chaves deve ser mantida em segredo.
Deve ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação estiver disponível.	Deve ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação esteja disponível.
Conhecimento do algoritmo mais as amostras do texto cifrado devem ser insuficientes para determinar a chave.	Conhecimento do algoritmo mais uma das chaves, mais as amostras do texto cifrado devem ser insuficientes para determinar a outra chave.

Fonte: Stallings, Willian (1999, p.167)

2.1.3.1 Principais Algoritmos Assimétricos

a) Diffie – Hellman – DH

Como citado anteriormente, o ponto de partida para a criptografia por chave pública se deu a partir do artigo publicado por Whitfield Diffie e Martin Hellman (Terada, 2002). O algoritmo DH não gera uma chave de sessão simétrica e a distribui utilizando a tecnologia de chave pública; em vez disso, a tecnologia de chave pública é utilizada para gerar a chave de sessão simétrica.

Cada participante possui um valor secreto e um valor público, se combinado um valor privado com outro público, cada participante gerará o mesmo valor secreto, que será usada para futuras comunicações. As chaves públicas e privadas estão relacionadas a cada um dos pares de chaves, como mostra a figura 8.

Segundo Burnett & Paine (2002), o algoritmo DH não criptografa os dados, ele somente gera um segredo. Dessa forma, as duas partes podem gerar um segredo e então utilizá-lo para criar uma chave de sessão para ser utilizada em um algoritmo simétrico. Este procedimento é chamado de acordo de chaves, onde as duas partes realizam uma troca, cujo resultado é uma chave compartilhada.

A técnica DH é baseada no Problema do Logaritmo Discreto. Uma chave Diffie-Hellman consiste em um gerador, um módulo e um valor público. A chave é o mesmo módulo do valor privado. Com o DH utiliza-se um único primo de 1.024 bits como módulo; por causa disso, ele não é tão complexo e seguro, se comparado com o algoritmo RSA.

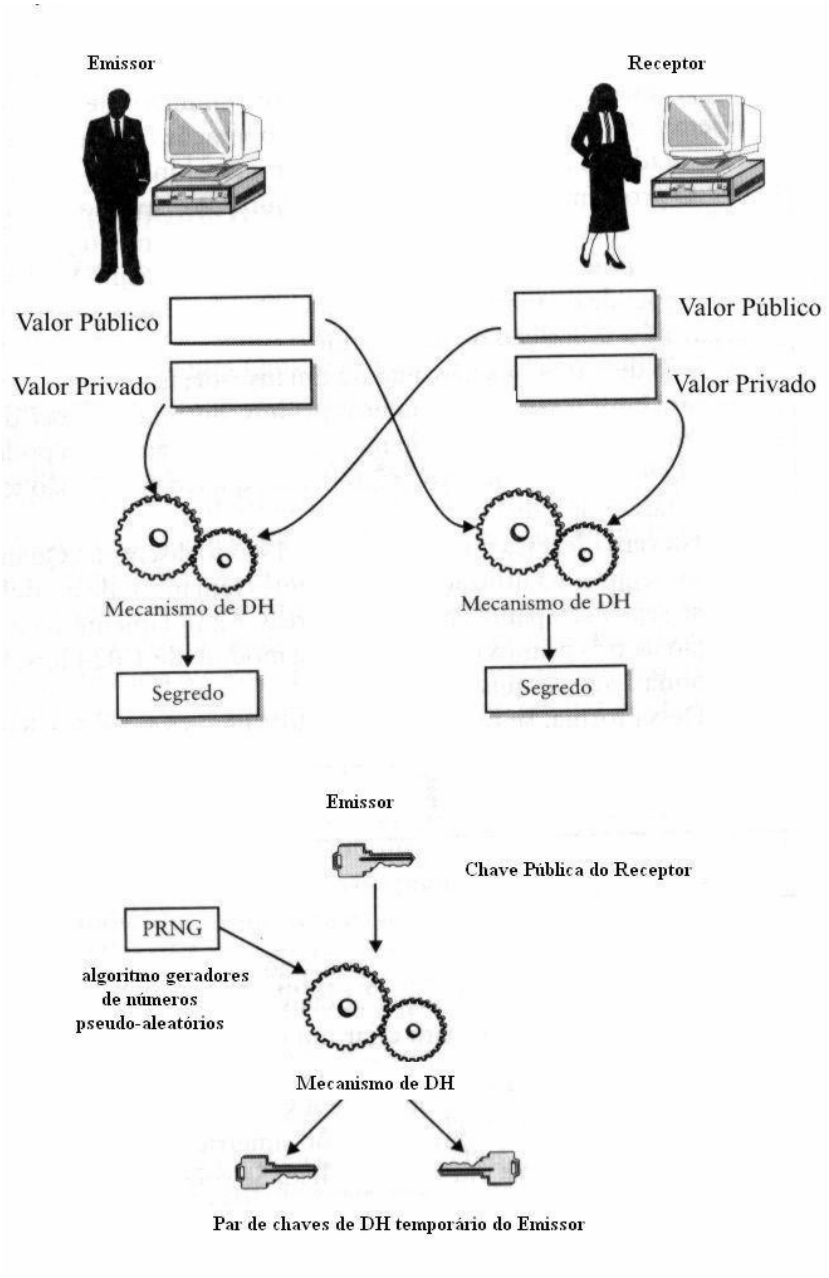

FIGURA 8 - Ilustração do algoritmo DH para gerar o mesmo valor secreto

FONTE: BURNETT, Steve; PAINE, Stephe. (2002, p.90).

b) RSA

O algoritmo RSA foi tornado público em 1978 por Ronald Rivest, Adi Shamir e Len Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T.). As iniciais RSA correspondem às iniciais dos inventores do código. (Coutinho, 2000).

O algoritmo tomou por base o estudo feito por Diffie e Hellman, porém usando outro fundamento matemático para a criação das chaves públicas. Ao contrário do

algoritmo DH, que utiliza um único primo de 1.024 bits como módulo e realiza o acordo de chave, o módulo de 1.024 bits do RSA é obtido através da multiplicação de dois números primos de 512 bits e criptografa os dados.

Segundo Terada (2000, p.101), o algoritmo RSA é baseado na dificuldade computacional de fatorar um número inteiro em primos, ou seja, a promessa por trás do RSA é que é fácil multiplicar dois números primos para obter um terceiro número, mas muito difícil recuperar os dois primos a partir daquele terceiro número.

Para implementar o RSA são necessários dois parâmetros básicos: dois números primos (*p* e *q*) e seu produto (*n*). A chave de codificação do RSA é constituída essencialmente pelo número *n*, sendo $n = p \cdot q$. Cada usuário do método possui sua chave de codificação, que é tornada pública (*n*), por isso *n* é conhecido como chave pública e a chave de decodificação é constituída pelos primos *p* e *q* (chave privada), que o usuário deve manter em sigilo, pois, caso contrário a segurança do método estará comprometida.

Se a fórmula $n = p \cdot q$ é conhecida, a princípio parece ser fácil descobrir *p* e *q*, a partir do número conhecido *n*, pois bastaria fatorar *n* para que o código fosse decifrado. No entanto, para se obter chaves de codificação seguras, é necessário que as mesmas sejam geradas por números muito grandes (com 150 algarismos ou mais).

Segundo Coutinho (2000, p.3), desde sua criação, o algoritmo RSA tem reinado como a única abordagem amplamente aceitável e implementável da encriptação de chave pública utilizando os princípios de uma expressão exponencial, aliados a conceitos dos números primos, aritmética modular e do Teorema de Euler.

O esquema de encriptação do algoritmo RSA é aplicado sobre blocos de tamanho máximo definido. Como a maioria das mensagens supera este tamanho, elas devem ser quebradas em fragmentos de tamanho apropriado.

É importante notar que, quanto mais avançadas forem as técnicas de fatoração, torna-se razoável admitir que não haverá modificação na utilidade destes algoritmos, pois os números primos são gerados pela utilização das mesmas técnicas. Logo, quanto mais fácil for fatorar um número de um tamanho específico, mais fácil será gerar primos de tamanhos maiores.

Considerando que a busca de fatores primos é um dos problemas mais antigos da matemática, sua utilização para um problema prático é considerada de grande

elegância. A matemática que estuda as propriedades dos números inteiros é conhecida como Teoria dos Números (Coutinho, 2000).

2.1.4 O controle sobre a criptografia

Devido à sua origem militar, e por sua função estratégica, a criptografia é altamente regulamentada em diversos países. As restrições quanto à importação e exportação da criptografia estão diretamente ligadas ao tamanho das chaves criptográficas (Oaks, 1999).

França e Israel, por exemplo, exercem forte controle não somente sobre a importação e exportação dessa tecnologia, mas também sobre sua utilização doméstica. O controle francês vê a criptografia acima de 40 bits como elemento crítico para a defesa nacional; assim, o tamanho máximo liberado para uso público não passaria de 56 bits, incapaz de garantir plena segurança aos dados que trafegam em redes abertas como a Internet.

Em Israel, a importação, exportação, produção ou uso de qualquer produto de criptografia exige licença do Ministério da Defesa.

A China, a exemplo dos dois países já citados, também exerce forte controle sobre os procedimentos criptográficos. A importação ou exportação desse tipo de produto exige licença governamental, tanto para uso doméstico como empresarial.

Na outra ponta dessa tendência de restrições à produção e uso dos sistemas criptográficos, estão países como Canadá, Finlândia, Alemanha e Japão, que consideram os sistemas criptográficos necessários para a proteção de dados pessoais, o desenvolvimento do comércio eletrônico e de todos os negócios confidenciais. Por isso, existe, nesses países, uma grande preocupação com os aspectos criminais que, eventualmente, poderão advir da disseminação da criptografia, ficando as autoridades responsáveis por monitorar o desenvolvimento da tecnologia e pela aplicação das leis que regulamentam essas atividades (Lucca & Simão Filho, 2000).

Na América Latina, Brasil incluso, essa questão não tem merecido maiores preocupações dos setores oficiais, apesar de haver um consenso sobre o fato de que a criptografia é uma importante ferramenta para a privacidade do cidadão em um mundo cada vez mais informatizado.

Nos Estados Unidos, a criptografia é considerada artigo de defesa e faz parte da "*Lista de Munições dos Estados Unidos*", estando relacionada na categoria "Equipamento Militar Auxiliar". Mesmo assim, não há restrições para seu uso doméstico

Segundo Burnett & Paine (2002), em janeiro de 2000, o governo dos Estados Unidos anunciou um relaxamento significativo quanto às restrições para a exportação de criptografia forte, permitindo assim que empresas norte-americanas possam competir mundialmente no setor de criptografia.

Para uma criptografia ser considerada forte, ela tem que mudar pelo menos 50% do resultado final ao ser alterado um caractere no texto original ou o mínimo possível na chave de criptografia. Segundo Schneier (2001), para a criptografia simétrica um tamanho mínimo recomendado é de 90 bits e para a assimétrica o tamanho é de 1.024 bits, além de cada país determinar o tamanho da chave que considera como "criptografia forte".

2.2 Biometria

Aceita pela primeira vez como método científico de identificação no final do século XVIII, a biometria, ou como era chamada na época, Antropometria, usava as medidas de partes do corpo na catalogação de tipos humanos. (Aical, 2001).

Atualmente a biometria é uma técnica comumente usada pelos computadores para determinar a identidade de uma pessoa, onde é feita uma medição física desta pessoa e comparara-se esta medida física com o perfil que foi previamente gravado. Esta técnica é chamada de *medida biométrica,* porque é baseada na medição das características de um ser vivo. (Garfinkel & Spafford, 1999).

Burnett & Paine (2002, pág. 242) descrevem a biometria como sendo:

> "a ciência utilizada para medir uma característica do corpo humano; em seu aplicativo comercial, tais medidas são utilizadas para verificar a identidade reivindicada de um indivíduo. As características físicas como impressões digitais, retina e íris impressões da mão"

Segundo Garfinkel & Spafford, (1999), existem duas maneiras por meio dos quais os sistemas de identificação de medida biométrica podem ser usados. O mais simples e mais confiável é comparar as medidas de um indivíduo com um perfil

específico que está armazenado. A segunda técnica é varrer um grande banco de dados de perfis armazenados e procurar uma coincidência específica.

Para a utilização inicial da biometria, cada usuário deve ser inscrito por um administrador de sistema, o qual verifica cada indivíduo que está sendo inscrito é um usuário autorizado. A característica biológica é obtida por um dispositivo de hardware, conhecido como *sensor,* que em geral reside no front end do mecanismo de autenticação biométrico. Depois que os usuários se inscrevem, suas biometria são utilizadas para verificar suas identidades, na autenticação de uma pessoa, a sua característica biológica é obtida no sensor e convertida em uma representação digital, chamada de *varredura direta*, onde é comparada com o modelo biométrico armazenado.

Assim como cada corpo humano tem inúmeras características únicas, inúmeros métodos de reconhecimento podem ser utilizados na biometria. A seguir serão descritos alguns métodos biométricos mais comuns de reconhecimento em utilização.

a) Reconhecimento de impressão digital

Essa forma de criptografia de dados evoluiu nas últimas décadas a partir do uso de impressões digitais para identificação. Neste modelo de biometria, a impressão digital de uma pessoa é varrida eletronicamente para decodificar informações, assim o transmissor dos dados pode ter certeza de que o destinatário é o receptor dos dados.

Segundo Burnett & Paine (2002), outro poder da impressão digital biométrica se deve ao fato de que as impressões digitais são mais amplamente aceitas, confiáveis e convenientes do que a identificação física, especialmente quando se utiliza tecnologia.

Este recurso biométrico possui um custo relativamente baixo, se comparado com os outros métodos disponíveis atualmente.

b) Reconhecimento óptico

Há dois tipos de biometria óptica: de retina e íris. Esses dispositivos são mais precisos do que os dispositivos de impressão digital e da palma da mão, pois, tanto

a retina como a íris tem mais características para identificar e corresponder do que as encontradas na mão. (Schneier,2001).

Aical (2001, p.02) descreve o funcionamento dos tipos de biometria óptica:

Leitura de retinas: neste método, os padrões dos vasos sangüíneos da retina são "lidos" por uma luz infravermelha com o auxílio de um leitor óptico. Os vasos absorvem mais rápido a luz que o tecido ao redor, formando uma imagem única que será analisada seguindo alguns pontos característicos. Esse método é bastante preciso, entretanto a técnica utilizada para se obter os dados é bastante inconveniente - a luz deve ser direcionada diretamente para a córnea; a obtenção de uma imagem correta da retina vai depender da habilidade do operador e da capacidade da pessoa que está sendo scaneada em seguir os procedimentos.

Leitura de íris: considerado menos intrusivo, esse método baseia-se nas características da íris dos olhos. O usuário deve manter-se à distância de 14 polegadas de uma câmera ccd (usada para criar imagens em bit map).

Há duas desvantagens quanto a estes dispositivos; eles têm dificuldade em ler imagens de pessoas cegas ou que tenham catarata, além de serem incômodos de utilizar, pelo menos nos modelos atuais. Um outro fator que os torna desinteressante é média de preços desses sistemas, que é de US$6.500,00 (Burnett & Paine,2002).

c) Reconhecimento facial

Esta forma biométrica, uma imagem é examinada em toda a estrutura facial. Freqüentemente, essa abordagem é menos confiável do que as formas mais comuns como varreduras de impressões digitais e íris. (Schneier,2001).

Segundo Aical (2001), dois padrões de tecnologia são aplicados. O escaneamento da imagem num padrão bidimensional - baseado na medida de ângulos e distâncias entre traços da fisionomia como olhos, nariz e boca. Essas medidas podem variar de acordo com o movimento do usuário.

O desenvolvimento da captura de imagens do rosto com uso do padrão tridimensional, entretanto, supre essa deficiência significando a percepção de mais detalhes, como a estrutura óssea ao redor dos olhos e do nariz. Uma vez capturada, a representação em três dimensões pode ser construída a partir de um simples frame de gravação de vídeo.

Para Burnett & Paine,(2002, p.246) um recurso atraente quanto aos produtos de reconhecimento facial é seu baixo custo, em geral, as unidades podem ser adquiridas por cerca de US$150,00. Com esse preço, essa tecnologia possa servir ao comércio eletrônico, mas as unidades podem ser incômodas de usar e, para propósitos de criptografia, ainda não são tão confiáveis quanto as outras formas biométricas.

d) Reconhecimento de voz

O reconhecimento de voz oferece várias vantagens para a utilização na criptografia. Não apenas a biometria da voz é perfeita em aplicativos de telecomunicações, mas também pelo fato de que a maioria dos computadores pessoais modernos já tem o hardware necessário para a utilizar esses aplicativos.

Segundo Burnett & Paine,(2002, p.246), os cartões de som podem ser adquiridos por cerca de US$50,00 e o preço para os microfones é cerca de US$10,00.

Esse tipo de reconhecimento envolve a gravação de um "modelo" para o padrão de voz que será usado na autenticação. O usuário deverá repetir determinada frase para que seu padrão de voz seja gravado.

Algumas desvantagens dessa tecnologia é que a gravação de voz pode variar no curso do dia e, se um usuário tiver um problema de saúde como uma gripe ou faringite, isso pode afetar a gravação.

e) Reconhecimento de assinatura

O reconhecimento biométrico de assinatura opera em um ambiente tridimensional que não se baseia apenas na comparação entre as assinaturas, mas sobretudo na dinâmica da assinatura do usuário, velocidade, direção, pressão e tracejado das letras.

A restrição desse método é que se baseia no padrão de comportamento. Nem sempre as pessoas assinam os documentos da mesma maneira. O ângulo que elas assinam pode ser diferente devido à posição em que elas sentam ou o posicionamento da mão na superfície, o que permite maior margem de erros na autenticação.

2.2.1 Problemas na utilização da biometria

Segundo Schneier (2001, p.148), a biometria é ótima porque ele é realmente difícil de falsificar , pois é difícil colocar uma impressão digital falsa de um dedo, ou fazer com que uma retina se pareça com a de outra pessoa. Por outro lado, a biometria é falha porque é muito fácil de se forjar: é fácil roubar uma biometria depois que a medição for feita.

Para Garfinkel e Spafford (1999), as medidas biométricas podem ser ferramentas confiáveis para a identificação precisa, mas eles oferecem tantos empecilhos para serem aplicados que acabam sendo deixados de lado. Alguns destes empecilhos incluem:

- Uma “impressão” biométrica de uma pessoa deve estar em um arquivo no banco de dados do computador antes que a pessoa possa ser identificada.
- A autenticação baseada em dados biométricos geralmente requer equipamento caro com a finalidade especial de medir o dado biométrico desejado.
- A menos que o equipamento seja especialmente protegido, ele é vulnerável à sabotagem e fraude.

Devido à possibilidade de falsas coincidências, as medidas biométricas são geralmente combinadas com senhas ou tokens. No caso das senhas, poderia ser requisitado ao usuário que digitasse um código de identificação secreto, com um número de identificação pessoal (PIN – personal identification number) e depois uma amostra do dado biométrico, como a gravação do trecho da voz. O sistema PIN para carregar o perfil específico que está armazenado, que é depois comparado com a amostra recém-adquirida

Atualmente, dispositivos biométricos não estão sendo utilizados de maneira disseminada, devido a algumas razões. Uma é o custo do dispositivo e a outro é a sua confiabilidade e desempenho, principalmente quando se refere à autenticação em um grande número de estações de trabalho, sua performance não é tão boa quanto deveria ser. Dependendo da quantidade de usuários em um banco de dados biométrico, a autenticação do usuário se torna lenta e inviável para utilização.

2.3 Assinatura digital

O conceito de assinatura digital é aplicado para documentos digitais da mesma forma que o conceito de assinatura comum é usado para documentos impressos; ambas autenticam a origem dos dados contidos naqueles documentos.

A assinatura escrita pode ser descrita como uma única combinação de traços de lápis ou caneta que seja bem difícil para outra pessoa qualquer forjar, e, com o passar do tempo, torna-se parte da identidade do indivíduo. (Volpi, 2001).

A assinatura comum, em certificados de empréstimos e outros documentos que podem ter poder jurídico, foi criada para proteger, contra a falsificação, um documento assinado. Igual finalidade têm documentos que utilizam marcas d'água, em alto relevo e / ou tratamento especial de tinta. Dessa forma, sua utilização garante que uma certa pessoa ou entidade escreveu ou está de acordo com o documento no qual a assinatura está colocada.

A assinatura digital pode ser entendida como uma identificação composta por números, que podem ser empregados como um meio efetivo na proteção de informações, estejam elas armazenadas em um computador ou sendo transmitidas pela rede. No segundo caso, a assinatura digital busca garantir que determinada mensagem não seja alterada durante seu trajeto. Além disso, ela busca resolver duas outras questões relacionadas à criptografia: a autenticação, que confirma a autenticidade da mensagem e a identidade de quem a enviou; e o não-repúdio, impedindo que pessoas retifiquem sua palavra eletrônica.

Baseado nesses dois princípios – a autenticação e o não-repúdio – as assinaturas digitais, assim como as assinaturas comuns, vêm sendo adotadas como um meio efetivo de provar judicialmente a autenticidade de um documento, como relatam Burnett & Paine (2002, p.117):

> "os governos começam a adotá-la, no nível estadual e nacional, estão sendo aprovadas leis que declaram uma assinatura digital como uma maneira de associar juridicamente a assinatura de documentos. Isso significa que qualquer coisa que seja encriptada com uma chave privada é uma assinatura digital."

Neste contexto, torna-se necessário explicitar a diferença entre uma assinatura eletrônica e uma assinatura digital. A primeira é um símbolo ou método qualquer, realizado por qualquer método de computador e é neutra quanto à tecnologia. O

simples ato de se digitar um nome em um e-mail pode ser considerado uma assinatura eletrônica, o que levanta sérias perguntas quanto à autenticidade do documento (Wadlow, 2000).

Já a assinatura digital refere-se a uma implementação de criptografia de chave pública, podendo ser definida como a transformação de um registro através da utilização de um sistema de chave pública, o que a torna mais confiável em muitos aspectos, como será visto adiante.

Segundo Volpi (2001), a assinatura digital é efetivada através de algoritmos de autenticação, através de um processo lógico-matemático aplicado sobre a mensagem a ser transmitida, criando, assim, uma determinada expressão que será utilizada como assinatura. A figura 9, abaixo, ilustra com maior clareza o funcionamento da assinatura digital.

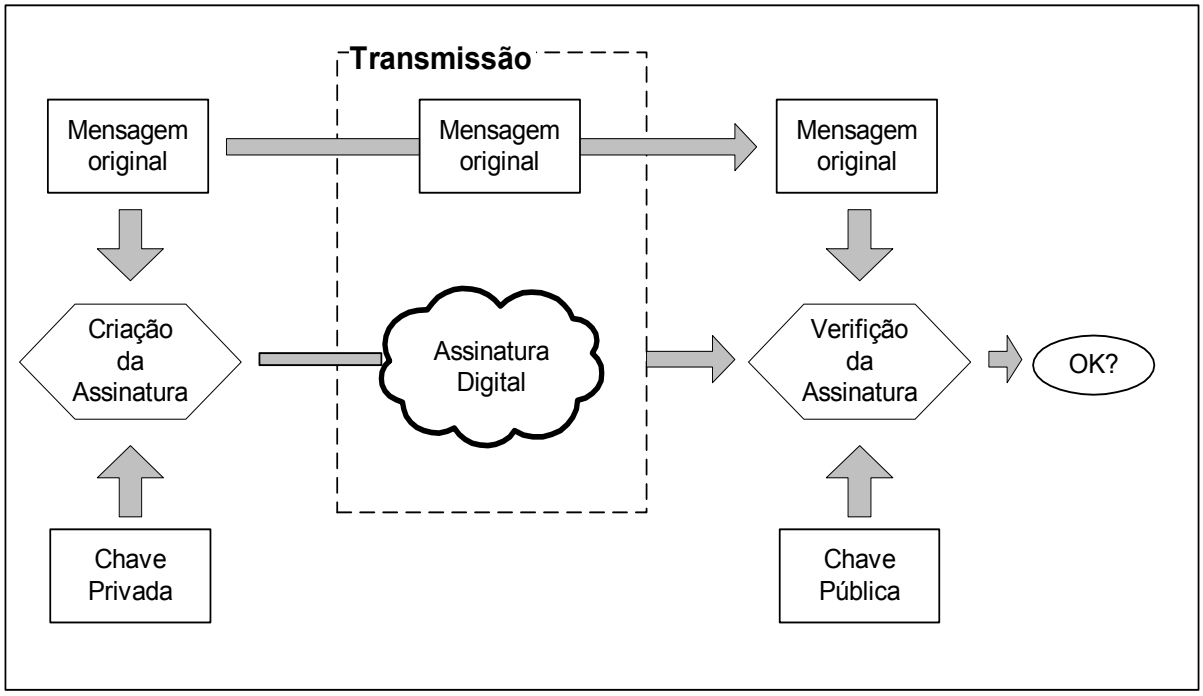

FIGURA 9 - Ilustração do funcionamento da assinatura Digital.

Fonte: VOLPI, Marlon M. (2001 p.17).

Conforme se vê na figura 9, a mensagem original é acompanhada de uma assinatura digital , baseada na chave privada do remetente. Quando a mensagem chega a seu destino, a assinatura é verificada, utilizando-se a chave pública que pertence ao remetente. Confirmada a assinatura digital a partir da verificação, pode-se ter a certeza da autenticidade da mensagem e do remetente.

É importante perceber que a assinatura digital, como descrita na figura anterior, não garante a confidencialidade da mensagem. Um interceptador poderá acessá-la e verificá-la apenas utilizando a chave pública do remetente. Para obter confidencialidade com assinatura digital, torna-se necessário combinar os dois métodos. O remetente primeiro assina a mensagem, utilizando sua chave privada. Em seguida, ele criptografa a mensagem novamente, junto com sua assinatura, utilizando a chave pública do receptador. Este, ao receber a mensagem, deve, primeiramente, decifrá-la com sua chave privada, o que garante sua privacidade. Em seguida, "decifrá-la" novamente, ou seja, verificar a assinatura utilizando a chave pública do remetente, garantindo assim sua autenticidade.

As assinaturas digitais dependem de duas suposições fundamentais: primeiro, que a chave privada seja segura e que apenas o proprietário da chave tenha acesso a ela (não existe nenhuma suposição técnica, exceto que as chaves devem ser protegidas), segundo, que a única maneira de produzir uma assinatura digital seja utilizando a chave privada. (Lynch, 1996).

Os fatores de risco, relacionados com os procedimentos de segurança, podem advir de motivos internos e/ou externos. Os principais motivos internos podem estar relacionados a problemas ocasionados por erros humanos ou mesmo a falhas técnicas; um bom exemplo disso é a corrupção do material do disco magnético. Com relação aos motivos externos podemos relacionar, principalmente, a interceptação no envio de documentos. Documentos estes, que podem ser alterados por terceiros, desviando assim o objetivo do mesmo. (Gomes, 2001).

Na atualidade, e com o objetivo de minimizar os fatores de risco, tem-se recorrido à utilização de senhas e chaves para realizar a assinatura digital de documentos como forma de garantir a autenticidade dos mesmos. As senhas e chaves são garantidas pelo emprego da criptografia e o uso de certas tecnologias, ligadas a cálculos matemáticos. Algumas dessas tecnologias são utilizadas em conjunto com outras com a finalidade de formarem assinaturas digitais mais consistentes (Volpi, 2001). Para se obter um maior entendimento do funcionamento da assinatura digital, serão descritas, abaixo, as técnicas mais utilizadas na criação da mesma.

2.3.1 Técnicas Aplicadas em uma assinatura digital

A assinatura digital obtida através do uso da criptografia assimétrica ou de chave pública, infelizmente, não pode ser empregada de forma isolada. A utilização isolada de algoritmos assimétricos para assinaturas digitais é inviável, principalmente quando se deseja assinar grandes mensagens, que podem levar muitos minutos ou mesmo horas para serem integralmente "cifradas" com uma chave privada, assim, o melhor método seria encripitá-las com um “representante de dados”.

2.3.1.1 Resumos de mensagem

Na criptografia, o representante de dados é um resumo de mensagem . A palavra “resumo” significa que para condensar, ou reduzir e ser suficientemente seguro, o arquivo que se queira enviar deve passar por um processo de “condensação”. Desta forma, é possível dizer que um resumo de mensagem é um algoritmo que recebe qualquer comprimento de entrada e mescla essa entrada para produzir uma saída pseudo-aleatória de largura fixa (20 bytes), freqüentemente chamada de função *hash*. A função *hash* pode significar desordem ou confusão, e descreve eficientemente o resultado de uma *message digest*. (Negroponte, 1995).

Como citado anteriormente, devido à lentidão dos algoritmos assimétricos – que, em geral, são cerca de 1.000 vezes mais lentos que os simétricos – a utilização da função *Hashing* como componente na implementação de assinaturas digitais, assim como para produzir um representante maior de dados é tão necessária que, quase sempre, uma chave de resumo torna-se imprescindível. (Schneier, 2001).

A função *Hashing* é uma espécie de uma impressão digital e serve, portanto, para garantir a integridade do conteúdo da mensagem que representa. Assim, após o valor *hash* de uma mensagem ter sido calculado através do emprego de uma função *Hashing*, qualquer modificação em seu conteúdo – mesmo em apenas um bit da mensagem – será detectada, pois um novo cálculo do valor *hash* sobre o conteúdo modificado resultará em um valor *hash* bastante distinto (Diniz, 1999). A probabilidade de duas mensagens diferentes produzirem o mesmo bloco deve ser praticamente nula, assim, a função *Hashing* oferece agilidade nas assinaturas digitais, além de integridade confiável.

2.3.1.2 Principais Algoritmos de Resumo

Segundo Burnett & Paine (2002) , existem vários algoritmos de resumo, mas três deles dominam o mercado atualmente: HMAC, MD2 e / ou MD5 e SHA-1, os quais serão descritos a seguir:

a) HMAC

O *Hashed Message Authentication Code* (Código de Autenticação de Mensagem Segura) é uma técnica que usa uma chave secreta e uma função de codificação para criar um código secreto de autenticação de mensagem. (Garfinkel & Spafford, 1999).

Segundo Burnett & Paine (2002, p.127):

> "MAC é o acrônimo de message authentication checksun (soma de verificação de autenticação de mensagem) ou message authentication code (códigos de autenticação de mensagem) e H significa hash; portanto um HMAC é um algoritmo de autenticação de mensagem baseado em hash e uma soma de verificação é um algoritmo que verifica os dados somando-os."

A figura 10 ilustra de que forma o algoritmo HMAC resume a chave e os dados para produzir um valor.

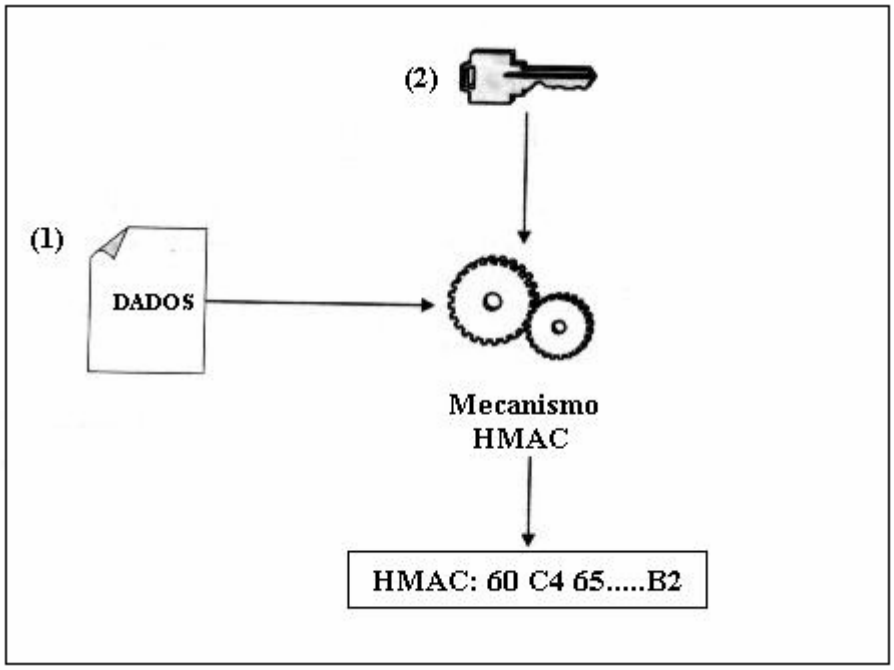

FIGURA 10 – Ilustração do algoritmo HMAC para produzir um valor.
Fonte: BURNETT, Steve; PAINE, Stephe (2002, p.128)

Como ilustrado na figura 10, duas partes compartilham uma chave secreta e então fazem um resumo de cada chave e mensagem. O resumo depende da mensagem e da chave, dessa forma um invasor teria de saber o que a chave é para alterar a mensagem e anexar a soma de verificação correta.

Se duas pessoas compartilham uma chave simétrica, é possível para uma delas, o remetente, executar um algoritmo simétrico, por exemplo o DES em cima dos dados, obtendo dessa forma, o código de autenticação da mensagem, e enviá-la juntamente com os dados. O receptor deverá estar apto para validar o código dos dados que lhe foram enviados; ele consegue isto realizando a mesma cifragem em cima dos dados recebidos e deve obter esse mesmo código. Se os dados foram adulterados, o receptor não obterá um valor que se iguala com o MAC enviado.

Obviamente que o atacante também pode modificar o MAC da mesma forma que pode modificar os dados. Porém, sem o conhecimento da chave utilizada para criar o MAC, não é possível para este modificar a informação enviada e depois computar um código que corresponda a mesma.

b) MD2 e MD5

Segundo Terada (2000, p.180), os algoritmos de resumo MD2 e MD5 foram desenvolvidos por Ron Rivest, e ambos são adaptações feitas por Rivest a partir do MD (o primeiro algoritmo de resumo de Rivest).

O MD2 produz um bloco de 128 bits (16-bytes) e, assim, existem 2.128 possíveis valores de resumo. Este algoritmo foi amplamente utilizado, mas, com o passar dos anos, os analistas encontraram defeitos nele, como algumas colisões em certas classes de mensagens. Portanto o MD2 não tem sido muito utilizado, exceto em certificados antigos.

Após as descobertas dos analistas das fraquezas no MD2, foram criados, por Rivest mais outros dois algoritmos de resumo: o MD3 e o MD4 que, logo após suas apresentações para o mundo, rapidamente tiveram suas fraquezas reveladas. Assim surgiu o mais bem sucedido algoritmo da geração MD, que foi o MD5.

Garfinkel & Spafford (1999, p.203), relatam que: “assim como o MD2, o MD5 é um resumo de 16 bytes, no entanto o MD5 mostrou-se muito mais seguro e mais rápido do que os anteriores e tornou-se o algoritmo dominante e ainda é comumente utilizado”.

Embora largamente usado, foram descobertas algumas falhas nele em meados de 1996. O MD5 ainda não foi quebrado e ninguém encontrou colisões; em vez disso, algumas partes internas do algoritmo são vulneráveis . Se faltasse um ou dois componentes no algoritmo, ele seria quebrado. (Oaks, 1999).

c) SHA-1

O SHA-1, surgiu de uma pequena modificação do seu antecessor, o SHA (*Secure Hash Algorithm*). Ambos foram desenvolvidos para utilização como padrão da assinatura digital pelo NIST – *National Institute for Standards Technology* (Instituto Nacional para Padrões e Tecnologia).

Segundo Burnett & Paine (2002, p.125), o algoritmo SHA-1 se parece muito com o MD5, no entanto suas partes internas são mais fortes por produzirem um resumo mais longo (160 bits comparados com 128 bits) e, por isso, é altamente recomendado pela comunidade criptográfica. Variantes do SHA-1 que produzem resumos de 192 bits a 256 bits ainda estão em desenvolvimento.

2.3.2 Como funciona uma assinatura digital

Conforme descrito anteriormente, a assinatura digital não pode ser gerada a partir do documento original; por isto, aplica-se sobre a mensagem um algoritmo de resumo.

Após analisar os principais algoritmos de resumo, o HMAC parece ser o mais viável para constituir uma assinatura digital. No entanto, ele contém algumas falhas. A primeira delas, é que não resolve o problema de não-repúdio, pois ambos, emissor e receptor, conhecem a chave para criar a chave HMAC correta. A segunda desvantagem é que, para o emissor e o receptor verificarem a “assinatura”, os correspondentes devem revelar a chave secreta, e se a mesma foi interceptada por um terceiro, este também poderá criar mensagens que parecerão ser genuínas.

As HMACs são utilizadas apenas para verificar se o conteúdo não foi adulterado durante o trânsito, elas se destinam a serem utilizadas como uma verificação instantânea e não como um registro permanente. (Schneier, 1996).

É importante notar algo poderoso quanto à assinatura digital: cada fragmento de dados tem sua própria assinatura. Isso significa que nenhuma assinatura digital é associada a uma pessoa ou a um par de chaves (Schneier,2001).

Segundo Burnett & Paine (2002, p.86):

> “Quando uma pessoa assina duas mensagens com a mesma chave , as assinaturas serão diferentes. Além disso, quando duas pessoas com chaves diferentes assinam os mesmos dados , elas produzirão assinaturas diferentes. Como resultado disso, alguém não pode pegar uma assinatura válida e acrescentá-la à parte de uma mensagem diferente.”

Existem, também, algumas outras verificações que podem ser feitas, como, por exemplo, aquela feita através de alguns bytes identificadores de algoritmos de resumo e alguns bytes de enchimento além dos de resumo. O verificador verifica não apenas o resumo mas também os bytes de enchimento e o identificador de algoritmo SHA-1. Os bytes do identificador de algoritmo evitam que um invasor substitua isso com um algoritmo de resumo alternativo (Lindeberg, 1999).

Para se construir uma assinatura digital realmente confiável, ou seja, garantir sua integridade contra ataques, é necessário amarrar essa assinatura com um resumo e com um algoritmo. (Diniz, 1999).

Segundo Burnett & Paine (2002, p.131), “as assinaturas digitais podem ser usadas para convencer um terceiro, o que resolve o problema de não-repúdio e para se criar assinaturas verificáveis a única maneira é encriptar o resumo com a chave privada do assinante.”

2.3.2.1 Principais algoritmos utilizados em uma Assinatura Digital

Existem vário algoritmos que são utilizado na criação de uma assinatura digital. Abaixo, serão descritos dois deles, o RSA e o DSA, que se colocam entre os principais algoritmos em uso.

a) RSA

Como visto anteriormente, o algoritmo RSA é um algoritmo de chave pública que encripta um resumo com uma chave privada e produz uma assinatura digital. A matemática utilizada é a mesma tanto para a administração de chaves quanto para assinaturas digitais. Para forjar uma assinatura RSA é necessário conhecer a chave privada. Sem uma chave privada, ninguém foi capaz de produzir um fragmento de dados, chamar isso de uma assinatura digital e fazer com que isso seja verificado. (Burnett & Paine, 2002).

b) Digital Signature Algorithm – DSA

Segundo Volpi (2001, p.26), o DSA (*Digital Signature Algorithm*) é o algoritmo base para o chamado DSS (*Digital Signature Standard*). Após uma fase de implantação, em que sofreu algumas poucas alterações, em 1994, veio a ser homologado pelo *Federal Information Processing Standard* (FIPS), tornando-se assim, o método de assinatura digital padrão aceito pelo governo americano.

O DSA utiliza um resumo de dados mas não o criptografa, assim, sua utilização se restringe a assinaturas digitais.

O assinante resume a mensagem com o SHA -1 e trata desse resumo como um número (160 bits de comprimento). Um outro número enviado ao algoritmo é um valor aleatório, chamado de *k* e a última entrada é a chave privada. Em seguida, o algoritmo realiza algumas operações matemáticas, uma das quais é a exponenciação modular. A saída são dois números, chamados de *r* e *s.* Esses dois números são a assinatura.

Utilizando o resumo como um número, junto com a chave pública e o *s*, o verificador realiza algumas operações matemáticas. O resultado dos cálculos é um número chamado *v*. Se *v* for igual a *r*, a assinatura é verificada – considerada autêntica. Esse procedimento é mostrado na figura 11.

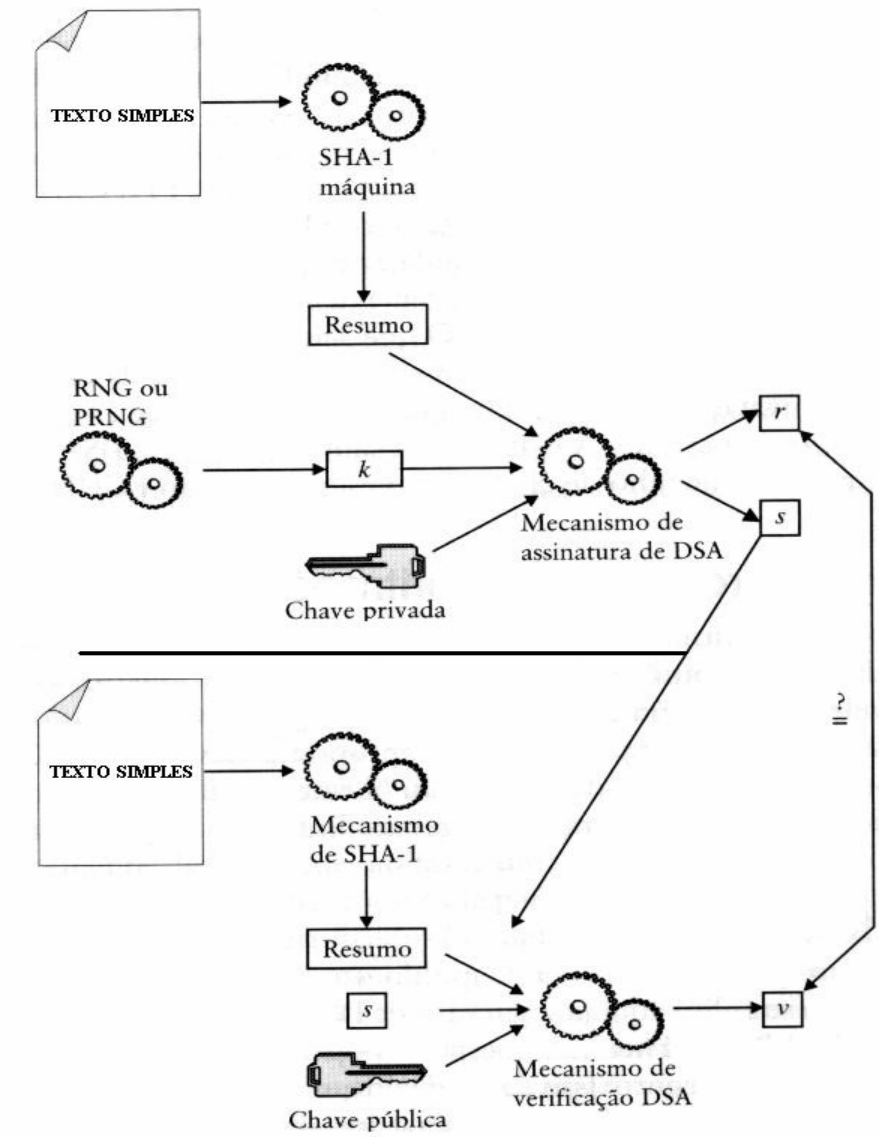

FIGURA 11 – Ilustração de um processo de criptografia utilizando o DSA.
Fonte: BURNETT, Steve; PAINE, Stephe (2002, p. 137).

A segurança do DSA reside no problema do logaritmo discreto, o mesmo problema que fornece a segurança ao DH. O tamanho das chaves geradas pelos algoritmos RSA e DSA são os mesmos (1.024 bits) (Oaks, 1999).

No que diz respeitos às semelhanças entre os dois algoritmos apresentados, Volpi (2001, p.28) declara que:

> "Para o usuário final, os métodos de assinatura digital RSA e DSS são muito semelhantes, tanto na segurança como no modo de operação. Os critérios a serem estipulados na hora da escolha entre um e outro devem levar em consideração aspectos de licenciamento, performance e aceitação pelo mercado onde será aplicado."

2.4 Patentes dos Algoritmos

As patentes aplicadas aos programas de computador são conhecidas como "patentes de software". Algumas das mais antigas patentes de software concedidas pelo Departamento de Marcas e Patentes dos Estados Unidos são relacionadas à criptografia.

Garfinkel & Spafford (1999) relatam que: "embora se acreditasse não ser possível patentear algoritmos computacionais, as patentes de criptografia foram aceitas, pois eram parentes de dispositivos criptográficos internos de hardware".

O sistema RSA de criptografia de chave pública é utilizado em diversos sistemas criptográficos como PGP, S/MIME, SSL, entre outros.(Abrantes, 2002). Em setembro de 2000, a patente do algoritmo RSA expirou e atualmente qualquer firma ou indivíduo pode criar implementações desse algoritmo.(Burnett & Paine, 2002). Apesar do algoritmo RSA ser amplamente recomendado e aceito pela comunidade criptográfica ainda existem restrições quanto a sua utilização em determinados países.

A tecnologia de chave pública é largamente adotada na Europa, onde é possível encontrar cartões telefônicos inteligentes, com dispositivos criptográficos e ampla disseminação dos algoritmos de chave pública. Isto se deve ao fato de que, no Japão e na Europa, o inventor perde o direito à patente após a primeira revelação. Já nos Estados Unidos, o inventor tem um período de carência de um ano entre a primeira revelação pública da descoberta e o pedido de patente.

Os algoritmos de criptografia simétrica RC2 e RC4, também desenvolvidos pela RSA Data Security, não foram objeto de patente, mas sim mantidos como segredo comercial. No DES e Triple DES não se aplica patente por serem padrão da NITS (National Institute of Standards and Technology) (Oaks, 1999).

O algoritmo DSA, por ser um algoritmo padrão de assinatura digital e ter licença livre, pode ser utilizado por qualquer pessoa, em qualquer país, pois, conforme relatado anteriormente, este algoritmo não criptografa os dados e sua finalidade se restringe às assinaturas digitais.

2.5 Certificados Digitais

Como visto anteriormente, quando um documento eletrônico é enviado ele trafega cifrado na rede ou contém uma assinatura digital, sendo esta gerada a partir de uma chave privada.

Para que a decifragem do documento seja feita, torna-se necessário que o receptor possua a chave pública, sendo esta gerada a partir da chave privada do emissor. De uma maneira mais ampla, a chave privada deve estar sob a posse de todos aqueles que poderão ter acesso às informações. Sendo uma ferramenta que permite somente a leitura, a chave pública não necessita ser confidencial.

Entretanto, o grande problema é que, como com quaisquer outros dados, uma chave pública é susceptível à manipulação durante o trânsito, desta forma um possível interceptador poderia alterar o documento original e até mesmo falsificar a assinatura digital.

Em uma população pequena de usuários confiáveis a distribuição poderia ser feita pelo método de distribuição manual de chave pública, entretanto em uma população geograficamente dispersa, este método torna-se inviável. Por esta razão, a solução foi a criação dos certificados digitais, que podem ser definidos como uma ligação entre uma chave pública e uma entidade (Lindeberg, 1999).

Um certificado digital é produzido de tal maneira que torna perceptível o fato – se vier a acontecer – de um impostor adquirir um certificado existente e substituir a chave pública ou o nome. Qualquer pessoa, ao examinar esse certificado, saberá

que algo está errado, portanto não confiará na combinação desse par de chaves e no nome.

Segundo Garfinkel e Spafford (1999, p.113), “a maneira mais comum de saber se uma chave pública pertence à entidade de destino é por meio de um certificado digital. Um certificado digital associa um nome a uma chave pública”.

Os certificados são emitidos para os usuários por terceiros, chamados autoridades certificadoras (Certification Authorities - CAs). Uma CA pode ser um departamento de segurança da empresa, um governo ou uma companhia privada que trabalhe com a emissão de certificados para usuários da Internet.

A certificação digital pode ser comparada a um serviço notarial efetuado pelo tabelião. Fundamenta-se na existência de uma CA que possui, registrada em sua base de informações, a chave pública do emissor do documento. Através de mecanismos próprios, a autoridade certificadora pode identificar como original o documento do emissor e, a partir desta comprovação, certificar, com uma assinatura digital própria, a autenticidade do documento eletrônico. (Diniz, 1999).

Burnett & Paine (2002, p.141), definem uma autoridade certificadora como sendo:

> “Uma organização, uma entidade independente e legalmente habilitada para exercer as funções de distribuição das chaves que pode ser consultado à qualquer tempo, certificando que determinada pessoa é a titular da assinatura digital , da chave pública e da correspectiva chave privada, sendo responsável pela emissão dos chamados certificados digitais.”

Vários certificados estão em utilização atualmente. Dentre eles, podem ser citados: o PGP (*Pretty Good Privacy*) – que é patenteado – e os certificados populares específicos de um aplicativo, como o de Transação Eletrônica Segura (*Secure Eletronic Transactions* – SET) e o Protocolo de segurança de Internet (*Internet Protocol Security* – IPSec). No entanto, o mais amplamente aceito é o X.509 – Versão 3, da *International Telecommunications Union* (Kurose & Ross, 2003).

O padrão X.509 foi publicado em 1988 e, desde então, foi revisado duas vezes – uma em 1993 e, novamente, em 1995. Um perfil para o padrão X.509, foi publicado em 1999 pela *Internet Engineering Task Force* (IETF) e, embora tenha sido criado para a comunidade da Internet, alguns de seus componentes podem ser aplicados em um ambiente empresarial.

Stallings, (1999, p.341) descreve uma estrutura para os certificados X.509, afirmando que todas as versões dos certificados X.509 contêm os seguintes campos:

- **Versão:** que diferencia as sucessivas versões do certificado;
- **Número serial de certificado:** que contém um valor inteiro único para cada certificado e é gerado pela CA;
- **Identificador do algoritmo de assinatura:** que identifica o indicador do algoritmo utilizado para assinar o certificado;
- **Nome do emissor:** com o nome distinto pelo qual a CA cria e assina aquele certificado;
- **Validade – Não antes / Não depois:** contêm dois valores de data/hora – que definem o intervalo temporal no qual um certificado pode ser considerado válido;
- **Nome do sujeito:** identifica o nome distinto da entidade final a que o certificado se refere, isto é, o sujeito que mantêm a chave privada correspondente;
- **Informações sobre a chave pública do sujeito:** contêm o valor da chave pública do sujeito, bem como o identificador de algoritmo de quaisquer parâmetros associados ao algoritmo pelos quais a chave deve ser utilizada.

A figura 12, abaixo, ilustra a estrutura dos certificados X.509 e seus respectivos campos, de acordo com cada versão:

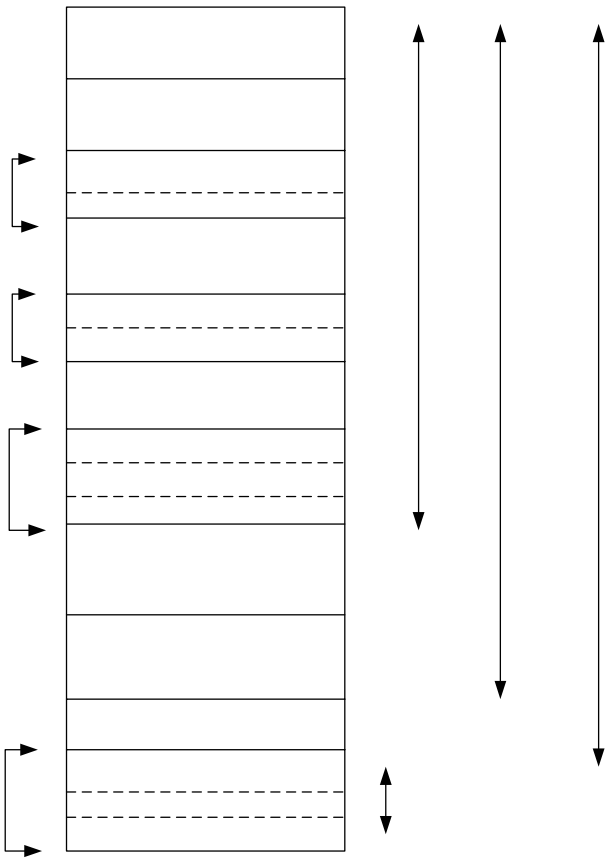

FIGURA 12 - Formato do certificado X.509

Fonte: STALLINGS, William (1999, p.342).

Segundo Garfinkel & Spafford (1999), um certificado X.509, em sua versão 3, certifica se uma chave pública foi assinada por uma instituição em particular. Essa certificação é selada por meio do uso de uma assinatura digital.

As CAs possuem uma hierarquia, sendo seu nível mais alto conhecido como "autoridades de certificação raiz" ou "infra-estrutura de chave pública" (*Public Key Infrastructure* - PKI)".

2.6 Componentes de uma Infra estrutura de chave pública – PKI

Segundo Burnett & Paine (2002, p.152), uma infra-estrutura de chave pública envolve um processo colaborativo entre várias entidades: a CA, uma autoridade de

registro (registration authority – RA), um repositório de certificado, um servidor de recuperação de chave e o usuário final.

2.6.1 Autoridade certificadora

Em uma PKI, uma CA emite, gerencia e revoga certificados para uma comunidade de usuários finais, assumindo as tarefas de autenticação dos seus usuários e assinando digitalmente as informações sobre o certificado antes de disseminá-lo. (Schneier, 1996)

Uma CA deve fornecer sua própria chave pública para todos os usuários finais certificados e para todas as partes verificadoras que possam utilizar as informações certificadas.

As CAs podem pertencem a duas categorias distintas: pública e privada. As CAs públicas operam via Internet, fornecendo serviços de certificação para o público em geral, certificando não apenas os usuários, mas também as empresas. Já as CAs privadas normalmente são encontradas dentro de uma corporação ou rede similar, e tendem a licenciar apenas usuários finais dentro da própria população, fornecendo assim controles de acesso e autenticação mais rigorosos. (Northcutt, et al, 2002).

Segundo Volpi (2001, p.36), as principais informações na emissão de um certificado são:

- Chave pública do autor.
- Nome e endereço de e-mail do autor.
- Data de validade da chave pública.
- Nome da autoridade certificadora que emitiu seu Certificado Digital.
- Número de série do certificado digital.
- Assinatura digital da autoridade certificadora.

No entanto é importante observar que somente algumas informações básicas estão contidas em um certificado digital e que existem vários formatos utilizados por diferentes autoridades certificadoras.

2.6.2 Autoridade registradora

À medida que aumenta o número de entidades finais dentro de uma comunidade de PKI, também aumenta a carga de trabalho de uma CA. Desta forma, uma RA (Autoridade Registradora) pode servir como uma entidade intermediária entre a CA e seus usuários finais, ajudando a CA em suas funções rotineiras para processamento de certificados, validando o que há no certificado. (Stallings,1999).

Levando em consideração o número crescente de usuários finais dentro de um domínio de uma PKI, é provável que eles se tornem geograficamente mais dispersos, desta forma, as CAs podem delegar a autoridade para aceitar as informações de registro de uma RA local.

Uma RA comumente aumenta a conveniência dos usuários finais, exercendo várias funções, tais como: aceitar informações de registros sobre novos registradores, gerar chaves em favor de usuários finais, aceitar solicitações para um *backup* e uma recuperação de chave, aceitar e autorizar solicitações para revogação de certificado e distribuir dispositivos de hardware como *tokens*, quando necessário. (Burnett & Paine, 2002)

2.6.3 Diretório de certificado

Após a geração de um certificado, ele deve ser armazenado para ser utilizado posteriormente. As CAs freqüentemente utilizam um diretório de certificado – ou uma localização central de armazenamento – que fornece um único ponto para a administração e distribuição de certificados. Esses diretórios atenuam a necessidade de que os usuários finais armazenem o certificado em máquinas locais.

Não há padrão requerido de diretório. Alguns aplicativos, como Lotus Notes e Microsoft Exchange, utilizam diretórios patenteados; atualmente, os diretórios baseados no padrão X.500 também estão ganhando popularidade. (Garfinkel & Spafford, 2000).

Para Northcutt *et. al*. (2002, p.619), os diretórios X.500 estão se tornando mais amplamente aceitos porque, além de atuarem como repositório de certificados, fornecem aos administradores uma localização central para entrada das informações de atributos pessoais. A acessibilidade às informações sobre o usuário é controlada a partir de diferentes clientes, utilizando para tanto um protocolo de acesso ao diretório.

Os clientes de diretórios podem localizar as entradas e seus atributos utilizando um protocolo de acesso ao diretório como o *Lightweight Directory Access Protocol* (LDAP), que foi projetado para fornecer aos aplicativos um meio para acessar os diretórios X.500.

Burnett & Paine (2002, p.154) ressaltam que:

> "Devido à natureza da autoverificação de certificados, os próprios diretórios de certificados não necessariamente têm de ser confiáveis, pois se um diretório for comprometido, os certificados ainda podem ser validados por meio de um certificado pela CA. Entretanto, se o servidor de diretório contiver dados pessoais ou corporativos, talvez seja necessário fornecer segurança e controle de acesso para ele."

2.6.4 Servidor de recuperação de chaves

Em uma população PKI, pode acontecer a perda de chaves privadas por parte dos usuários finais, seja por falha de hardware, senha esquecida ou qualquer outra eventualidade que venha a acontecer posteriormente. Qualquer que seja o motivo, este implicará em um grande problema para a PKI.

Caso o usuário perca a chave privada, a CA deverá revogar o certificado de chave pública correspondente e gerar um novo par de chaves, desta forma todos os dados encriptados antes do incidente tornam-se irrecuperáveis. (Schneier, 2001). A solução encontrada para este tipo de problema foi o servidor de recuperação de chaves. Ele fornece à CA uma maneira simples para fazer um *backup* de chaves privadas, no momento de sua criação, e a permite sua recuperação posterior. Algumas CAs suportam dois pares de chaves: um para criptografia e outro para assinatura e verificação.

Em relação ao gerenciamento de múltiplas chaves, ou seja, vários certificados para diferentes propósitos, Burnett & Paine (2002, p. 170) relatam que:

> "Uma chave privada que for utilizada para fornecer assinaturas digitais com propósito de não repúdio requer um armazenamento seguro por toda vida útil da chave. Durante sua vida útil, não há nenhum requisito para fazer backup; se a chave for extraviada, um novo par de chaves deve ser gerado. Depois que a vida útil da chave expirar, a chave não deve ser arquivada. Em vez disso, ela deve ser seguramente destruída."

2.6.5 Revogação de certificado

As CAs, além de emitirem certificados, estabelecem métodos para tirá-los de circulação. Isso acontece em virtude de vários fatores, tais como: uma chave privada perde sua validade, um certificado pode ter sido emitido para uma pessoa ou entidade incorreta, dentre outros (Diniz, 1999). Desta forma, as CAs precisam de uma maneira para revogar um certificado em vigor e notificar as partes verificadoras sobre a revogação.

O método encontrado foi o da criação de uma lista de revogação de certificados (*Certificate Revocation List* – CRL) (Schneier, 2001). Em sua forma básica, uma CRL é uma estrutura de dados assinada contendo uma lista de data/hora dos certificados revogados.

Após criar uma CRL e assiná-la digitalmente, o assinante de uma CRL – em geral a mesma CA que originalmente a emitiu – a distribui livremente, através de uma rede, ou a armazena em um diretório, da mesma forma que os certificados são tratados. Cabe às CAs emitirem periodicamente CRLs, que podem variar desde algumas horas até algumas semanas. No entanto, uma nova CRL é periodicamente emitida, contendo ou não novas revogações, permitindo que as partes verificadoras sempre saibam das revogações mais atuais (Wadlow, 2000).

Garfinkel & Spafford (1999, p. 115), declaram que:

> "Em vez de CRLs, a maioria das CAs de produção provavelmente usarão a verificação em tempo real utilizando sistemas de gerenciamento de banco de dados conectados à uma rede como a Internet. Estes sistemas resolvem basicamente os problemas envolvidos na CRL, ainda que eles precisem de uma rede que seja confiável e esteja disponível."

Uma das formas de se lidar com o problema dos certificados revogados é limitar a quantidade de tempo na qual eles possam ser usados, ou seja, com prazo de expiração bastante curtos – um a dois minutos (Schneier,2001).

2.7 Problemas na construção de uma PKI

A utilização de PKI atuando como um terceiro confiável na emissão de certificados para assinaturas digitais parece ser, até o momento, a forma mais segura de reduzir as chances de se fraudar uma chave, uma vez que basta ao destinatário o conhecimento da chave pública única da CA (Volpi, 2001).

No entanto, é importante observar que a utilização de uma PKI apresenta alguns problemas na sua construção, que serão relatados para que seja feita uma análise da necessidade (ou não), da sua utilização como um terceiro confiável.

Em uma PKI, a integridade da infra-estrutura depende da segurança das chaves de criptografia particulares; assim, o requerente do certificado deverá gerar, com segurança, a sua chave privada, utilizando um sistema confiável e tomando as precauções necessárias para evitar seu comprometimento. Os computadores atuais não são seguramente indicados para armazenar as chaves particulares depois de terem sido geradas. Assim, a forma mais segura de armazenagem encontrada nos dias atuais é a da implementação de cartões de PC de alto padrão para todos os usuários, gerando um alto custo na construção de uma PKI; de qualquer forma, um usuário final está completamente sob o controle dos demais usuários finais. Isto significa que os usuários, e não a Autoridade Certificadora, são os responsáveis pelo uso fraudulento das chaves, o que levanta dúvidas sobre o valor da declaração de responsabilidade por uma chave declarada por uma CA.

Como citado anteriormente, os usuários que tiverem suas chaves comprometidas deverão informar o fato às CAs, para que as partes verificadoras tomem conhecimento da revogação, através de uma CRL. No entanto, Burnett e Paine (2002, p.158) argumentam que:

> "A latência entre CRLs é uma desvantagem importante para a sua utilização, pois uma informação de uma revogação não pode ser recebida pela parte verificadora até a próxima emissão de uma CRL, o que pode durar várias horas ou semanas mais tarde."

Devido à ausência de padrão, auditorias e sistemas formais de aprovação na criação de CAs, o usuário que optar por uma determinada "empresa", deverá confiar nas regras de certificação da mesma quando inclui nela sua assinatura, ou seja, deverá julgar digno de crédito seu regime de práticas e garantias.

Segundo Garfinkel & Spafford (1999), mesmo que as CAs fossem corporações totalmente honestas e íntegras e que nunca cometessem erros, outro ponto desfavorável em relação é o fato de que nomes não são pessoas e, desta forma, um

certificado deveria conter mais do que simplesmente o nome da pessoa registrada na CA; ele deveria conter informações suficientes para identificar legalmente e de forma única um indivíduo, como por exemplo, um que portasse um nome comum como, por exemplo, José Pereira.

Apesar das características desfavoráveis relatadas na construção de uma PKI, em alguns países onde a assinatura digital certificada é equiparada a uma assinatura autografada, podendo ser considerada “evidência probatória” – evidência que é útil para determinar a identidade que pode ser usada nos tribunais (Lucca & Simão Filho, 2000) – a CA torna-se de suma importância, exercendo o papel de terceiro confiável.

Os criptógrafos definem um terceiro confiável como sendo alguém de confiança a qualquer um envolvido em um protocolo para ajudar a completar o protocolo de forma justa e segura.

Schneier (2001, p.228), relata que:

> “sistemas seguros aproveitam os terceiros confiáveis inerentes aos sistemas que eles estão protegendo. Sistemas mal projetados introduzem terceiros confiáveis sem entender as ramificações na segurança. Sistemas terrivelmente projetados são obrigados a usar terceiros confiáveis por lei.”

No primeiro caso (sistemas seguros), o próprio banco de dados de chave pública poderia servir como um terceiro confiável, levando em consideração os aspectos relacionados a segurança do sistema. O segundo e o terceiro caso, poderiam ser solucionados utilizando os serviços prestados por empresas que dão suporte as assinaturas digitais e de autoridades certificadoras como a VeriSign.

A VeriSign, foi o primeiro órgão de certificação a oferecer serviços públicos da Web, constituindo-se em uma autoridade certificadora que emite certificados de chave pública a usuários finais (Kurose & Ross, 2003). É uma empresa que presta serviços de identificação, autenticação, validação e pagamento em redes de comunicação. Permite que pessoas físicas e jurídicas, em qualquer lugar do mundo, se comuniquem, transacionem e comercializem com segurança em meio eletrônico, controlando mais de 5 bilhões de conexões de redes e transações por dia.

2.8 Emprego da assinatura digital

No decorrer da história, os principais eventos mundiais foram consumados pelo simples ato de assinar papéis. Assim, com o incremento das transações em redes de informação, as assinaturas digitais ganham relevo e desempenham um papel importante no desenvolvimento das tecnologias atuais.

Por serem únicas, as assinaturas identificam os indivíduos de forma inegável, permitindo a autenticação de importantes transações e mantêm as empresas e os indivíduos conectados ao mundo palpável do papel e da caneta.

Hoje, o advento das assinaturas digitais está modificando a maneira de conduzir negócios virtuais, possibilitando a identificação e a assinatura de documentos legais. As assinaturas digitais permitem que usuários de dispositivos eletrônicos validem a identidade e autentiquem documentos utilizando como ferramenta a tecnologia digital.

Burnett e Paine (2002, p.251), relatam que:

> "Graças à Internet, o comércio eletrônico alterou significativamente nossa maneira de fazer negócios. Com o passar dos dias, as transações baseadas no papel - incluindo acordos de poder jurídico – estão se tornando obsoletos à medida que o uso de acordos eletrônicos transmitidos pela Internet cresce em popularidade. O principal motivo dessa alteração é a conveniência."

Também é aceito sem questionamento o fato de que as experiências dos usuários com assinaturas digitais mostraram que essa tecnologia pode economizar tempo e dinheiro para as partes envolvidas, se comparadas à assinatura em papel

Quase sempre as assinaturas digitais na Web são codificadas, usam os níveis mais elevados de codificação e são praticamente invisíveis para o usuário final. Cada vez que um cartão de crédito é utilizado para uma transação na Web, no envio e recebimento de mensagens ou até mesmo em documentos legais, existem grandes chances de que haja alguma forma de tecnologia de assinatura digital validando e dando segurança à transação (Albertin, 1999).

2.8.1 Comércio eletrônico

Atualmente, a compra e a venda de produtos aplicados à rede não são feitas de maneira tradicional, pois estão se tornando totalmente automatizadas. Os clientes podem acessar lojas virtuais, escolher produtos, bens e serviços e tirar dúvidas em

tempo real, utilizando as mais diversas tecnologias. É possível, por exemplo, fazer cotações de preços, acessar contas bancárias a partir de terminais domésticos, dentre outras transações.

Assim como os clientes, as empresas também se beneficiam com essa nova tecnologia , associando a ela, ferramentas e softwares que garantam a segurança no momento da transação (Lucca & Simão Filho, 2000).

O comércio eletrônico engloba todas as atividades realizadas para vender produtos ou serviços através da Web, assim como todas as práticas e processos facilitados pelas redes de computadores, sendo visto como o conjunto de todas as transações comerciais efetuadas por uma empresa "pontocom". Esse tipo de empresa tem por objetivo atender, direta ou indiretamente, seus clientes, utilizando as facilidades de comunicação e de transferência de dados mediadas pela Internet.

Drucker (2000, p.112) relata um trecho do boletim do estudo anual da IDC Brasil para a América Latina, afirmando que:

> “o número de internautas brasileiros deve somar este ano 5,7 milhões, fatores como o acesso gratuito e o aumento da base instalada de micros motivaram o instituto a atualizar os números do estudo. A entrada do acesso gratuito aumentou entre 10% e 15% a comunidade de usuários de Internet no Brasil durante os dois primeiros meses deste ano.”

Com o volume crescente de compras e vendas na Web, surge a necessidade de proteger as transações on-line. As assinaturas digitais podem fornecem esta segurança. O comércio eletrônico, ao aceitar a assinatura digital e se beneficiar com sua utilização, busca segurança em sua atividade. Por catalisar o crescimento da tecnologia, em virtude da lógica inerente ao sistema capitalista, uma vez que as empresas “pontocom” se sintam mais seguras, a disponibilidade de serviços on-line deverá aumentar.

As transações comerciais eletrônicas são bastante semelhantes às transações comerciais tradicionais. Os produtos são apresentados no site da empresa, bem como os preços e as formas de pagamento e os prováveis compradores avaliam as opções, formas de pagamento e efetuam o pedido. Após confirmação da compra, a empresa envia o produto adquirido ao cliente.

Segundo Volpi (2001, p.33) para garantir a fidelidade, tanto da empresa quanto do comprador, o sistema da empresa é controlado na assinatura digital descrita em dois modelos:

Modelo Formalista: Não há preocupação quanto à segurança da assinatura, tanto a tecnologia aplicada na assinatura como a legislação que a regulamenta seriam estáticas, é possível dizer que faz-se necessária a confiança mútua entre a empresa e o comprador, não existindo um documento que ateste contrato. Apesar do baixo custo, a aplicação deste modelo não se torna viável no contexto atual.

Modelo " risck-based": A preocupação com a segurança é o foco principal, a assinatura eletrônica requer autenticações específicas que evitem o repúdio da autoria, essas precisam ser dinâmicas, com nível de segurança proporcional ao conteúdo da transação, garantindo a fidelidade e a autenticidade da ocorrência. O custo envolvido neste modelo aumenta consideravelmente em relação ao modelo formalista, e mesmo com o mesmo nível de segurança, dois documentos diferentes do mesmo remetente recebem assinaturas digitais distintas, uma vez que a assinatura é elaborada com base no conteúdo assinado.

2.8.2 Transações bancárias

Desde 2001 foi determinado que seja instituído o Sistema de Pagamentos Brasileiros (SPB), o qual exige que os bancos brasileiros utilizem a assinatura digital no processo de compensação bancária, com o intuito de garantir mais segurança e agilidade às transações e informações que circulam pela Internet entre o Banco Central e as outras instituições financeiras.

Essa determinação se deu após o Governo ter definido as regras de atuação da Infra-estrutura de Chaves Públicas (ICP), ou seja, a tecnologia que vai gerar as Assinaturas Digitais.

É com base nesse dispositivo que alguns bancos comerciais vêm implementando sistemas de assinatura eletrônica, utilizando senhas ou mesmo certificados digitais, mesmo sem a necessária certificação pela Autoridade Certificadora-Raiz brasileira.

Com o objetivo de proteger o cliente e estimular as transações on-line, os bancos estão lançando programas de certificação digital, buscando aumentar a segurança das transações bancárias feitas via Internet. A estratégia dessas instituições é de atingir contas corporativas e seus prepostos, funcionários dos próprios bancos e demais correntistas.

Uma das vantagens da certificação digital é que, após a sua emissão, o correntista passa a assinar digitalmente as suas transações, podendo efetuar qualquer tipo de transação enquanto estiver conectado à Internet (Certisign, 2003).

Os clientes devem fazer sua adesão à Certificação Digital oferecida pelos bancos imprimindo o termo de adesão, obtido no site da instituição, ou dirigindo-se pessoalmente à agência bancária. Em ambos os casos, a liberação do Certificado para uso na Internet só acontece após a conferência da assinatura manual dos clientes, nas agências detentoras das contas. Após a conferência da assinatura, é enviada ao cliente uma mensagem eletrônica, avisando-o da liberação para uso.

O Regulamento constitui-se na utilização do atributo de segurança, denominado Certificado Digital, que identifica o cliente e promove a autenticidade de suas transações via Internet, junto aos bancos. O certificado digital irá conter: a chave pública de criptografia, data de validade da chave pública de criptografia, nome e assinatura digital da entidade certificadora, o número de série do certificado digital, emissão do certificado digital e os dados cadastrais do cliente (Certisign, 2003).

A validade do certificado é de doze meses, contados a partir da data de sua emissão, a qual estará registrada, juntamente com a data de seu vencimento, no próprio certificado digital do cliente; sua revogação poderá ser feita a pedido do cliente e a qualquer tempo.

O certificado digital será revogado quando: o sigilo da senha pessoal de acesso tenha sido violado, houver perda, destruição ou impossibilidade de recuperação do certificado digital e, em último caso, quando não houver mais interesse em utilizar o certificado.

Após a adesão à certificação digital, o cliente deverá, obrigatoriamente, utilizá-la para acesso aos produtos e serviços do banco disponibilizados via Internet. Em qualquer tempo, o cliente poderá copiar o seu certificado digital do computador onde estiver instalado, para outros computadores ou qualquer outra mídia, conferindo portabilidade ao certificado.

Por sua vez, os bancos devem garantir a impossibilidade de emissão de certificados digitais com número de série idêntico ao de qualquer outro certificado que tenha sido emitido sob as regras firmadas em contrato do banco com a entidade certificadora. Além disso, devem disponibilizar, via Internet, orientações e meios para que o cliente possa solicitar a emissão, revogação e renovação do seu certificado digital.

Os bancos poderão, a qualquer tempo, introduzir modificações no Regulamento, mediante prévia e tempestiva divulgação aos clientes e registro em Cartório.

O Regulamento dos bancos deverá estar registrado em Cartório de Registro de Documentos da cidade de Brasília DF e arquivado em cópia microfilmada.

No que diz respeito aos clientes, os mesmos deverão requerer proteção especial do tipo antivírus, antitrojans e antihackers que garantam a inviolabilidade do certificado digital, sendo de responsabilidade do cliente manter tais programas atualizados no seu computador.

2.8.3 Atos jurídicos

Desde que a Internet se tornou um meio um meio eficaz de comunicação entre pessoas civis e jurídicas, a questão da segurança tornou-se presente como elemento garantidor do sucesso dessas atividades e, em função deste elemento, ressurgiram os modos de cifrar as mensagens, de forma que apenas o remetente e o receptor possam ter acesso ao teor dos documentos envolvidos na transação, garantindo o sucesso dessas relações. Desta forma, uma das mais importantes transformações, na área jurídica, se deu na conceituação de Documento.

A expressão "documento", sempre esteve atrelada à idéia de um escrito oficial que identifica uma pessoa. No meio jurídico, representa um escrito que faz fé daquilo que atesta, de forma que, se apresentado em juízo, prova o que o litigante alega (Lucca & Simão Filho, 2000).

Com o advento da Internet e a sua rápida expansão pelo mundo, o conceito de documento teve que passar por uma adequação, de forma a se tornar viável a sua aplicação ao meio virtual, tendendo a alcançar os mesmos objetivos já consolidados no meio tradicional.

Dentro dessa nova conjuntura, surgiu, então, a conceituação do Documento Eletrônico, que guarda as principais características do Documento Tradicional, excetuando-se o meio no qual é celebrada uma transação e a questão atinente à identificação da pessoa. É possível conceituar o Documento Eletrônico como sendo a representação não material de um fato, tendente a alcançar segurança jurídica.

Criando um paralelo entre as duas conceituações, é possível dizer que a principal diferença dos documentos tradicionais com os documentos eletrônicos é que o primeiro é representado por escritos em papéis e o segundo por bits.

É unanimemente reconhecida a necessidade de se dar eficácia e validade jurídica aos contatos virtuais, de modo que possam ser equiparados aos documentos conhecidos atualmente, que estão ligados a um meio material tangível.

Entre os diversos novos recursos que foram colocados à disposição dos usuários de computadores, a comunicação eletrônica tem recebido a adesão da quase totalidade dos advogados, substituindo em grande parte a comunicação que antes era feita por postal e pelo fac-símile.

A comunicação eletrônica decorre das inúmeras vantagens em relação à comunicação tradicional. Burnett e Paine (2000, p.251), descrevem as principais vantagens, nos seguintes tópicos :

- **Integridade de mensagem:** uma assinatura digital é superior a uma assinatura escrita à mão, pois ela atesta o conteúdo de uma mensagem e a entidade do assinante.
- **Economia:** o uso de sistemas abertos (como a Internet) como mídia de transporte pode ajudar consideravelmente a economizar tempo e dinheiro. Além de adicionar automação significativa, possibilita que os dados sejam assinados digitalmente e enviados de uma maneira oportuna.
- **Armazenamento:** os dados de negócios (contratos e documentos semelhantes) podem ser armazenados muito mais facilmente em uma forma eletrônica do que na forma de papel. Um documento que foi assinado digitalmente pode ter validade indefinida, devido ao registro de data/hora que permite provar a validade de um contrato mesmo se, em algum momento, a chave do assinante for comprometida depois que o contrato já estiver assinado.
- **Diminuição de erros:** Se adequadamente implementadas, as assinaturas digitais reduzem o risco de fraude e tentativa por uma parte de repudiar (negar) o contrato.

Vários estudos estão sendo feitos por diversos organismos ligados à administração da Justiça visando dar os primeiros passos para a criação do “processo virtual”, cujo objetivo consiste basicamente em possibilitar que o processo seja desenvolvido totalmente a partir de documentos eletrônicos, muitos deles

enviados por meio de comunicação eletrônica (Kaminski, 2002). Desta forma, a comunicação eletrônica constitui um instrumento cada vez mais importante para o exercício da advocacia, tanto na comunicação entre o advogado e o cliente, quanto na evolução da comunicação entre o advogado e os órgãos do poder público.

As assinaturas digitais permitem a realização de inúmeros atos jurídicos à longa distância, possibilitando uma enorme flexibilização das relações que necessitam serem concebidas de maneira expressa. Esta capacidade precisa estar devidamente regulamentada para que possa gozar de total confiança por parte daqueles que a utilizarão (Diniz,1999).

Um exemplo da aplicabilidade deste sistema pode ser verificado, no Brasil, analisando o funcionamento do governo federal, que vem utilizando o sistema de transmissão eletrônica de atos normativos entre os ministérios e a Presidência da República. A partir da implantação desse sistema automatizado e em tempo real, com toda tramitação acontecendo via Internet, a agilidade da administração federal só vem crescendo. Os documentos recebem a assinatura digital dos ministros e são enviados para conhecimento do presidente.

Em outros países, isto também já vem acontecendo. Na França, por exemplo, o governo utiliza sistema semelhante a esse, mas a tramitação dos documentos se dá na rede interna do governo (Intranet), que só é acessada em computadores de órgãos públicos. No Brasil, a Intranet Governamental ainda está em processo de implantação.

Em fevereiro de 2002, a OAB-SP, começou a operar sua certificadora em fase de testes públicos e os advogados de São Paulo puderam testar a assinatura digital. Em Abril de 2002, o Conselho Federal da Ordem dos Advogados do Brasil aprovou o Provimento que institui o ICP-OAB, o que tornou oficial a certificação digital dos advogados.

O projeto ICP-OAB vem sendo desenvolvido na Ordem dos Advogados do Brasil desde o ano 2000 porque a própria OAB preferiu ser a entidade certificadora dos advogados e, para tanto, precisou desenvolver seu próprio sistema para garantir a integridade das informações e restringir o acesso aos dados unicamente à Ordem. Inicialmente a implantação do sistema se dará no Conselho Federal, e, posteriormente, deverá ser expandida para todas as seccionais (Kaminski, 2002).

A principal vantagem da assinatura digital é a integridade da informação e a identificação virtual confiável, além de facilitar o trabalho dos profissionais, que

poderão fazer tudo eletronicamente. Um advogado que precisar peticionar junto a um órgão de Brasília poderá fazê-lo à distância. Dessa forma, os advogados avançam de forma consistente na informatização do Judiciário.

Kaminski (2002), relata que:

> "com a certificação devidamente regulamentada, qualquer documento eletrônico é revestido de validade jurídica, quer seja um contrato ou uma mensagem de e-mail comum. Caso o emitente e o receptor estejam portando certificados, é possível a utilização da criptografia de dados objetivando um maior sigilo."

2.9 Abordagens legislativas

Conforme relatado anteriormente, as assinaturas digitais oferecem uma série de benefícios para os negócios. No entanto, para que as mesmas se tornem mais prevalecentes, Burnett & Paine (2002, p.253), destacam duas barreiras que devem ser vencidas:

1. oferecer aos documentos existentes na forma eletrônica o mesmo status jurídico dos documentos do papel;

2. fornecer um método confiável, seguro e sancionado juridicamente para "assinatura" de documentos eletrônicos, que eliminará a necessidade de gerar e assinar documentos em papel. Com isso, será encorajado e facilitado o comércio eletrônico e o trâmite de documentos em repartições públicas.

Ambos os problemas requerem soluções legislativas e, naturalmente, devem ser acompanhadas pelo Direito, sob pena de as leis se tornarem estranhas à realidade social, cujo desenvolvimento deve ocorrer lado a lado ao desenvolvimento das ciências jurídicas.

A organização que representa a profissão jurídica nos Estados Unidos, a ABA (*American Bar Association*), tem feito um trabalho considerável com relação aos aspectos jurídicos das assinaturas digitais (Northcutt *et al*, 2002). O documento intitulado "*Digital Signature Guidelines*", foi publicado em 1996 pelo *Information Security Committee*, *Section of Science and Technology*.

Digital Signature Guidelines são diretrizes projetadas para fornecer declarações abstratas e gerais de princípios destinadas a servir como uma base unificadora, a

longo prazo, de uma lei para a assinatura digital em diversos documentos legais (Albertin, 1999). Após a divulgação dessas diretrizes, vários estados americanos escolheram modelar sua própria legislação sobre assinatura digital.

2.9.1 Conceitos jurídicos relacionados às assinaturas digitais

Para que os documentos eletrônicos contendo uma assinatura digital tenham a mesma validade jurídica dos documentos que possuem uma assinatura comum, torna-se necessário provar para um terceiro imparcial (um foro ou um juiz), que o conteúdo do documento eletrônico é genuíno e que foi originado pelo remetente. É necessário ainda, que o remetente não possa negar futuramente o conteúdo do documento que contém a sua assinatura digital.

Em outras palavras, volta-se aos conceitos de não-repúdio e autenticação, que, segundo Gomes (2001), desempenham um papel chave na legalidade das assinaturas digitais.

Como já descrito anteriormente, para Garfinkel & Spafford (1999, p.209) o não-repúdio pode ser considerado como sendo uma função que previne que o autor de uma mensagem negue o envio e/ou recebimento de uma mensagem; e a autenticação pode ser considerada uma forma que garante a identidade de quem está enviando a mensagem pois o receptor da mensagem pode verificar a identidade da pessoa que a assinou.

No que diz respeito aos conceitos jurídicos relacionados com as assinaturas digitais o não-repúdio e a autenticação abrangem um âmbito bem mais amplo,.

Segundo Burnett & Paine (2002, p.254), “o não-repúdio em documentos eletrônicos deve ser uma evidência irrefutável que pode ser mostrada em um foro judicial.” Os autores afirmam, ainda, que os serviços de não-repúdio, fornecem evidências confiáveis de que uma ação específica ocorreu e pode ser dividido em três tipos:

- **Não-repúdio de origem:** protege o destinatário de uma comunicação garantindo a identidade de quem originou uma comunicação. Confirma ainda a data/hora em que a mensagem foi enviada e a sua integridade (garante que o conteúdo da mensagem não foi modificado a transmissão).

- **Não-repúdio de entrega:** protege o remetente de uma comunicação garantindo a identidade de quem originou uma comunicação e também confirma a data/hora em que a mensagem foi enviada e a sua integridade.
- **Não-repúdio de submissão:** é semelhante ao não-repúdio de origem e de entrega, exceto que ele é utilizado para proteger o remetente contra qualquer reivindicação pelo destinatário de que os dados não foram enviados ou não foram enviados em uma data/hora específica.
- Quanto ao serviço de autenticação, para o propósito deste trabalho, Burnett & Paine (2002), relatam dois tipos de autenticação: autenticação de assinante e autenticação de dados.
- **A autenticação de assinante:** garante que o assinante tem ciência do conteúdo do documento que está assinando, para que o mesmo possa ter poder legal. Essa assinatura além de indicar quem assinou impossibilita uma outra pessoa de reproduzir a assinatura sem uma autorização.
- **A autenticação de dados:** garante que nenhuma modificação futura possa ser feita em um documento após o mesmo já ter sido assinado. Normalmente a autenticação de dados é acompanhada pela *autenticação de origem de dados*, a qual associa uma pessoa real a um documento específico.

Existem várias questões importantes que devem ser resolvidos para que a atual legislação de assinatura digital suporte um teste de litígio. Além dos conceitos de não-repúdio e autenticação e as diretrizes da *"Digital Signature Guidelines*", é necessário incorporar eficazmente as assinaturas digitais dentro de uma empresa ou repartição que sejam capazes de criarem e manterem uma infra-estrutura de chave pública (PKI) confiável (Gomes, 2001). Desta forma, uma PKI, necessariamente, deve estar envolvida em um processo colaborativo entre várias entidades: a CA, e uma RA, um repositório de certificado, um servidor de recuperação de chave e o usuário final, como já descritos anteriormente (Burnett & Paine, 2002).

Outro conceito relevante é o denominado "data/hora", que, segundo Schneier (2001, p.232), "é um conjunto de técnicas que permite determinar se um documento foi criado ou assinado em uma determinada (ou antes) data/hora."

Na maioria das vezes os sistemas de registro de data/hora utilizam um terceiro confiável, chamado de autoridade registradora de data/hora (*Time-Stamping Authority* – TSA). Esse serviço é de grande importância no que diz respeito aos

conceitos jurídicos relacionado às assinaturas digitais, possibilitando uma autenticação a longo prazo de documentos digitais. Por exemplo, se o assinante de um documento vier a revogar seu certificado após ter assinado um documento, é possível provar que o mesmo foi assinado antes que a chave correspondente da assinatura fosse revogada.

2.9.2 Regulamentação da assinatura digital

Há algum tempo a legislação da assinatura digital tem sido uma questão constante no mundo. Isso decorre do número crescente de transações comerciais internacionais, habitualmente conhecido como "comércio eletrônico".

A primeira iniciativa, em legislação, sobre a assinatura eletrônica ocorreu no ano de 1995, no estado de Utah (Estados Unidos), onde foi sancionada a primeira lei estadual referente à assinatura digital, que ganhou notoriedade na arena jurídica.

Em março de 1996 ela foi retificada e é amplamente reconhecida como o primeiro passo no reconhecimento jurídico da tecnologia de assinatura digital. O objetivo principal da legislação da assinatura digital do estado de Utah é de promover o desenvolvimento de uma infra-estrutura de chave-pública.

Na legislação vigente no estado de Utah são detalhados os direitos e as responsabilidades das partes em uma transação que utilize a criptografia de chave pública. O Estado oferece a licença de Autoridades certificadoras pelo Utah Department of Commerce, e as CAs que obtêm a licenças são tratadas com regras de responsabilidade favoráveis (Bernstein et al, 1997).

Outros estados norte-americanos começaram a levar em consideração leis modeladas de acordo com a lei de Utah, como, por exemplo, os estados de Washington e Geórgia. No entanto, mais tarde, esses e alguns outros estados permitiram que os projetos de lei morressem, optando por um estudo mais aprofundado. Outros estados adotaram métodos menos reguladores e específicos de tecnologia. Burnett & Paine (2002, p.259) exemplificam a aplicação das assinaturas digitais nesses estados da seguinte forma:

> “A Califórnia e o Arizona sancionaram uma legislação permitindo o uso de assinaturas digitais em transações que envolvem entidades estaduais. Essa legislação autorizou os dois secretários desses estados a promulgar

> regulamentos para alcançar o propósito de tal decreto. Outros ainda aprovaram leis permitindo o uso de assinaturas digitais para propósitos específicos como registros médicos ou para propósitos de orçamento e contabilidade como a verificação de assinatura digital pela secretaria da fazenda."

A importância de se regularizar a assinatura digital tornou-se ainda mais expressiva quando, em 1996, a União Européia adotou a lei da Comissão das Nações Unidas sobre o Direito do Comércio Internacional (*United Nations Commission on International Trade Laic* - UNCITRAL), que se tornou uma lei modelo sobre o comércio eletrônico, que serviria de referencial aos países-membro (Volpi, 2001).

Segundo Burnett & Paine (2002, p.259), "a lei modelo UNCITRAL é de alto nível, permitindo um método para as assinaturas e registros eletrônicos sem nenhuma menção quanto às assinaturas digitais ou a criptografia".

No que se refere especificamente à atuação da assinatura digital, a lei modelo descreve que, quando uma lei requisitar a assinatura de uma pessoa, este requisito será considerado preenchido por uma mensagem eletrônica quando:

- for utilizado algum método para identificar a pessoa e indicar sua aprovação para a informação contida na mensagem eletrônica;
- e tal método seja tão confiável quanto seja apropriado para os propósitos para os quais a mensagem foi gerada ou comunicada, levando-se em consideração todas as circunstâncias do caso. Incluindo qualquer acordo das partes a respeito.

Volpi (2001, p. 46) declara que:

> "Quanto às leis destinadas a regulamentar situações que envolvam aspectos tecnológicos, devem restringir-se somente aos princípios que norteiam esta tecnologia, pois, de outra forma, corre-se o risco de criar verdadeiros entraves legais para a evolução da matéria."

Na Europa, as leis para assinaturas digitais estão em vigor há mais de uma década. A Alemanha já tem a sua "*Informations Und Kommunikationsdienste Gesetz Lukdg*", lei Federal que estabelece condições gerais para o uso das assinaturas digitais, quanto a seu aspecto de segurança que se baseia no sistema de Criptografia (Lucca & Simão Filho, 2000).

E assim, outros países, como a Itália e a Bélgica adotaram procedimentos semelhantes. A ONU, por meio da comissão chamada UNCITRAL (Comissão das Nações Unidas sobre o Direito do Comércio Internacional) já volta os seus olhos para essa questão da segurança nas relações cibernéticas e reconhece os certificados emitidos por uma entidade certificadora de outro Estado membro da União Européia, se este possuir um grau de segurança equivalente ao dos países membros da ONU (Albertin, 1999).

A Lei de Assinaturas Eletrônicas no Comércio Nacional e Global (*Eletronic Signatures in Global And National Commerce* - E-SIGN) é um projeto de lei para assinaturas eletrônicas, criado após longas negociações entre o Senado e o Congresso dos Estados Unidos.

O *E-SIGN Act* foi assinado pelo ex-presidente Bill Clinton em 30 de junho de 2000 e se tornou lei efetiva em 1° de outubro de 2000 (Northcutt, 2002). Foi originalmente projetada para impulsionar o comércio eletrônico da Internet, eliminando trabalho em papel que advém de contratos. Essa legislação dá reconhecimento e efetiva juridicamente as assinaturas.

A legislação denominada E-SIGN fornece o importante fundamento para a viabilidade e aceitação legal de assinaturas digitais e tecnologias de comércio eletrônico associadas, em todas as regiões dos Estados Unidos. Os princípios estipulados na E-SIGN, oferecem a arquitetura necessária para expandir a adoção dessas tecnologias, assim como de diretrizes legais para sua utilização.

Baseados na lei E-SIGN, alguns serviços foram projetados para o suporte das assinaturas digitais, serviços de autoridades certificadoras, registro de data/hora e de tabelião digital, tais como:

- **VeriSign –** conforme já relatado, é uma CA que emite certificados de chave pública aos usuários finais em qualquer lugar do mundo (Kurose & Ross, 2003).
- **CertSign** – oferece os mesmos serviços que a VeriSign, por ser a sua única afiliada brasileira.
- **DigSign –** é uma empresa que já começou a vender os seus serviços digitais de registro de data/hora e de tabelião (Burnett & Paine, 2002, p.265).

Os profissionais da área jurídica devem se preparar para se tornarem tecnicamente bem informados. E espera-se que esse número aumente à medida

que outros casos jurídicos relacionados começarem a emergir no futuro (Garfinkel & Spafford,1999).

2.9.3 Regulamentação da assinatura digital no Brasil

A ciência do direito é, por natureza, uma ciência social, porém, paradoxalmente, é conservadora. Isso implica grande dificuldade de se assimilar prontamente as inovações sociais, principalmente no que diz respeito à autenticação eletrônica e à aplicação da assinatura digital em documentos (contratos, certidões, entre outros), que possam ter valor jurídico mediante a utilização de tal tecnologia.

Se, no passado, havia tempo adequado para que o direito captasse as modificações nos hábitos e costumes da sociedade, e, ainda assim, havia certa dificuldade em acompanhá-las, atualmente, em plena era da informação, a dificuldade é incontestavelmente maior.(Bittencourt,2002).

No entanto, devido à rapidez dos avanços tecnológicos atuais e das inúmeras e diversas transações efetuadas utilizando-se a Internet como meio, a integração dos profissionais ligados à tecnologia de informação, à matemática e à área jurídica torna-se de suma importância para que as facilidades oferecidas possam ser aproveitadas da melhor forma pela sociedade em geral, garantindo segurança e respaldo jurídico à ela.

Atualmente, no Brasil, existem vários estudos que visam a regulamentação da assinatura digital e alguns projetos que buscam abordar a matéria de forma mais precisa já estão tramitando no Congresso Nacional (Lucca & Simão Filho, 2000).

A Normatização da assinatura digital se efetivou legalmente no Brasil, com a criação de um regulamento para a sua utilização pelo Poder Executivo Federal.

Com o intuito de viabilizar a circulação de documentos e informações entre os órgãos do governo, com maior garantia de segurança e confiabilidade, o Poder Executivo Brasileiro criou, em 5 de setembro de 2000, o Decreto N.º 3.587, regulando o uso de sistemas de assinaturas digitais pelas autoridades governamentais, do primeiro ao terceiro escalão do governo.

Apesar de ter sido um primeiro passo para a aprovação dos demais projetos que se encontram em tramitação, o decreto N° 3.587 está direcionado para uma

tecnologia específica, o que não possibilita uma eventual flexibilização legal quando da ocorrência da evolução no meio tecnológico.

Alguns pontos relevantes do decreto em questão podem ser destacados, tais como, o ICP-Gov (Infra-estrutura de Chaves Públicas do Poder Executivo Federal). Trata-se de um conjunto de especificações (arquitetura, organização, técnicas, práticas e procedimentos) que visa à operacionalização de um sistema de certificação. Essa operacionalização é restrita ao método de cifragem assimétrica.

Dentro do ICP-Gov, criou-se a figura de uma AGP (Autoridade de Gerência de Políticas), organismo destinado a estabelecer os padrões (técnicos, operacionais e de segurança) a serem seguidos pelas CAs que seriam ligadas ao próprio ICP-Gov.

Cabe à AGP a criação de uma Autoridade Certificadora Raiz (AC Raiz), responsável pela emissão e manutenção dos certificados das CAs de órgãos da Administração Pública Federal e das CAs privadas credenciadas, bem como o gerenciamento da Lista de Certificados Revogados (CRL) (Certisign, 2003).

As RAs (Autoridades de Registro), também devem cumprir com suas responsabilidades em relação às CAs, responsabilidades estas já descritas anteriormente.

Um fator a ser considerado é que as CAs podem receber seu credenciamento em níveis diferenciados, de acordo com a finalidade na qual se proponham a atuar. No entanto as mesmas devem seguir critérios estabelecidos pela AGP. Esses padrões incluem aspectos técnicos internacionalmente reconhecidos e aspectos adicionais, tais como: plano de contingência, política e plano de segurança, análise de riscos, capacidade financeira da proponente e histórico no mercado. Em se tratando de uma CA privada, devem ser avaliados, ainda, antecedentes e histórico no mercado, além da cobertura jurídica e do seguro contra danos que a mesma fornece aos seus usuários.

Em relação ao decreto N° 3.587 Volpi (2001, p. 48) declarando que:

> “Mesmo sendo uma regulamentação direcionada ao ambiente interno do governo, esse Decreto tem uma grande virtude no que tange à abertura de uma nova situação, onde alguns fatos que já existiam no contexto prático, através da disponibilidade tecnológica, começam a ser amparados pelo meio jurídico.”

Atualmente, existem três projetos de lei no Congresso Nacional que abordam o tema assinatura digital.

Projeto de Lei do Senado N.º 672 de 1999 – este projeto segue o modelo de lei da UNCITRAL, de 1996, que procura regulamentar o comércio eletrônico de forma geral. Assim, pouco contribui para a assinatura digital especificamente. A abordagem deste projeto não estipula detalhadamente a tecnologia a ser utilizada. O fator principal desconsiderado pelo legislador refere-se ao fato de que existe, no meio da tecnologia de informação, uma série de elementos externos que podem vir a influenciar no conteúdo de um documento, e que a legislação não pode deixar ao encargo das partes a obrigação de possuírem conhecimentos técnicos suficiente para estipularem o meio que irá autenticar a operação.

Projeto de Lei da Câmara N.º 1.483 de 1999 – este projeto foi criado visando instituir a fatura eletrônica e a assinatura digital nas transações de comércio eletrônico. No que diz respeito à assinatura digital, visa objetivamente à validação do mecanismo para as transações comerciais eletrônicas. Quanto à forma de reconhecimento da assinatura, propõe que a mesma seja feita por órgão público, sem contudo especificar qual e como será o procedimento a ser adotado para a operacionalização do feito. O projeto em questão apresenta um aspecto excessivamente abstrato, buscando meramente regulamentar a existência da assinatura digital no país e remetendo a responsabilidade de estipular normas de funcionamento e controle para outros setores do Estado. No entanto, pode ser considerado de grande relevância, por ter iniciado um processo de mobilização do Poder Legislativo para a criação de uma regulamentação que ordene e controle a utilização da assinatura digital no Brasil (Volpi, 2001).

Projeto de Lei da Câmara N.° 1589 de 1999 – este projeto de Lei foi elaborado a partir do anteprojeto de lei desenvolvido pela comissão especial de informática jurídica da OAB-SP e dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital. Trata-se de um projeto muito mais extenso e que busca atender um universo muito maior de situações que se remetam a esta matéria. Encontra-se nele inserido uma vasta regulamentação sobre o tratamento legal do comércio eletrônico, bem como dos documentos eletrônicos. Por essa razão será tratado com mais profundidade aqui.

Logo em seu início, o projeto busca orientar para que a interpretação seja feita considerando-se o fato de que o comércio eletrônico opera inclusive de maneira internacional e que seja levado em consideração o dinâmico processo de evolução que existe no meio tecnológico. Desta forma, busca favorecer a existência de uma sobrevida a esse tipo de comércio caso haja uma eventual alteração no mercado internacional ou mesmo no meio tecnológico.

A eficácia do projeto é direcionada objetivamente para o sistema assimétrico de assinatura, entendendo como original o documento que apresente assinatura mediante mecanismo criptográfico de chave pública.

Segundo o projeto, passa a ser presumido como verdadeiro o conteúdo do documento eletrônico, desde que apresente uma assinatura digital, seguindo todos os atuais princípios da tecnologia que envolve as assinatura digitais. Assim, a assinatura digital deve:

- ser única e exclusiva para o documento assinado;
- ser passível de verificação;
- ser gerada sob o exclusivo controle do signatário;
- estar de tal modo ligada ao documento eletrônico que, em caso de posterior alteração deste, a assinatura seja invalidada;
- não ter sido gerada após a expiração, revogação ou suspensão das chaves;
- considerar como data do documento eletrônico a data em que foi registrado, a data da sua apresentação em repartição pública ou em juízo, ou, ainda, a data do ato ou fato que estabeleça, de modo certo, a anterioridade da formação do documento e respectivas assinaturas.

A figura do tabelião está presente no projeto que o responsabiliza pela emissão dos certificados digitais públicos. Assim como os Tabeliões convencionais, a atuação desses Tabeliões, no que diz respeito às assinaturas digitais e aos documentos eletrônicos, está ligada às mais diversas situações, inclusive fé perante terceiros. Desta forma é dotado de fé pública, possuindo, em sua essência, a função de garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos.

Volpi (2001, p.55) relata que:

> “Ao buscar junto ao tabelião a tarefa de garantir a autenticidade dos documentos eletrônicos perante terceiros, o projeto promove a manutenção do serviço notarial, dotado de fé pública e relacionado diretamente com o Estado. Este posicionamento figura de maneira interessante para a

> sociedade, uma vez que a responsabilidade da autoridade certificadora permanece diretamente vinculada ao poder público e não sob domínio exclusivo de uma entidade particular qualquer."

Segundo Lucca & Filho (2000, p.407), o projeto de lei estabelece as informações mínimas que o certificado digital deve conter e que seriam:

- identificação e assinatura digital do tabelião;
- data de emissão do certificado;
- identificação da chave pública e do seu titular, caso o certificado não seja diretamente apensado àquela;
- elementos que permitam identificar o sistema de cifragem utilizado;
- nome do titular e poder de representação de quem solicitou a certificação, no caso de o titular ser pessoa jurídica;
- a inclusão do prazo de validade do certificado;
- o número de série do certificado.

Cabe ao Poder Judiciário, mediante parecer técnico favorável emitido pelo Ministério da Ciência e Tecnologia (entidade responsável pela regulamentação dos aspectos técnicos do exercício de atividade de certificação eletrônica pelos tabeliães), efetivar as seguintes medidas:

- emitir autorização ao tabelião para que o mesmo possa exercer a atividade de certificação eletrônica;
- fiscalizar de forma legal e de sancionar sobre os tabeliães e seus oficiais;

No projeto em questão fica clara a grande responsabilidade que cabe ao Ministério da Ciência e Tecnologia, levando-se em consideração que o mesmo emitirá certificados para chaves de assinatura a serem utilizadas pelos tabeliães para formarem os certificados digitais. Desta forma, este serviço exige extrema especialização técnica, devido ao ritmo dinâmico de atualização dos aspectos de segurança.

Lucca & Filho (2000, p.415) declaram que:

> "Para regular o setor, poderia ser criada uma agência federal de certificação, a ser constituída, por exemplo, em conjunto pelo Poder Judiciário e pelo Ministério da Ciência e Tecnologia, com poder de polícia, função de analisar os pedidos de autorização para funcionamento, estabelecer regras e parâmetros para o exercício dessa atividade, sobre a tecnologia empregada etc. dever."

Ainda no que diz respeito à certificação digital, Volpi (2001, p.59) relata que:

> "Quanto ao tratamento da certificação digital, ressalta-se que o assunto é relacionado a um meio intangível, onde a confiança é depositada sobre informações que foram geradas a partir da computação de dados. Sob este aspecto, o projeto apresenta um ponto forte quando trata da fácil possibilidade da revogação ou suspensão da validade de um certificado digital."

O tabelião, segundo aquele projeto de lei, irá revogar ou suspender o certificado digital quando:

- o titular da chave de assinatura ou de seu representante solicitarem;
- de ofício ou por determinação do Poder Judiciário, caso seja verificado que o certificado foi expedido baseado em informações falsas;
- se tiver encerrado suas atividades, sem que tenha sido sucedido por outro tabelião;
- houver ocorrência de dúvida sobre a legitimidade do requerente ou no que diz respeito à segurança da chave privada do titular.
- No que diz respeito às responsabilidades dos tabeliões, o projeto de lei estabelece, dentre outras, as seguintes atribuições:
- Publicar os certificados digitais, a fim de facilitar a verificação por parte dos usuários que necessitarem desta informação, que deve ser em tempo real e mediante acesso eletrônico remoto;
- Permitir o acesso do público a todas as chaves por ele certificadas.

Caso o tabelião venha a encerrar suas atividades, deverá assegurar que os certificados que tenha emitido sejam transferidos para outro tabelião, e, na eventualidade de não haver sucesso na transferência, cabe ao tabelião revogar os referidos certificados. Deverá ele, ainda, enviar ao Poder Judiciário as fichas de pedido de certificação que foram preenchidas pelos requerentes na época da inscrição e as demais documentações inerentes às fichas.

O não cumprimento dessas responsabilidades acarretará penalidades que podem ser impostas aos tabeliães, na mesma forma daquela que aborda as sanções penais relacionadas a fatos sujeitos à sanção de outros crimes já tipificados pelo Código Penal.

Quando se refere à possibilidade de falsificação do documento eletrônico, o projeto determina que o documento eletrônico é falso quando:

- assinado com chaves fraudulentamente geradas em nome de outrem;
- acontecer de o documento ser alterado sem que a chave original tenha sido modificada; nesse caso, será solicitada ajuda técnica, utilizando para tanto, um algoritmo de codificação de maior vulnerabilidade, para que se prove a autenticidade do documento.

Devido à importância da matéria do Projeto de Lei 1589, de 1999, que vai afetar a vida de milhões de brasileiros, Lucca & Filho (2000, p.415) afirmam que o mesmo:

> "deveria estar melhor apresentado para que a sociedade civil organizada pudesse opinar, formular críticas e sugestões, a fim de aprimorar as propostas nele albergadas, adequando-o aos interesses e às necessidades dos setores público e privado, bem como da população em geral".

Todos os projetos citados anteriormente podem não refletir a regulamentação final sobre o assunto, entretanto, fornecem um forte direcionamento sobre como o tema será abordado na legislação do Brasil. (Volpi,2001)

3 MODELAGEM DA ASSINATURA DIGITAL EM JAVA

As redes eletrônicas abertas, como a Internet, têm assumido uma importância crescente na vida dos cidadãos, dos agentes econômicos, das Instituições e demais setores da sociedade moderna, proporcionando uma cadeia de relações que promovem os inter-relacionamentos globais. Com o advento da Internet, modificou-se substancialmente a maneira pela qual são estabelecidas as relações entre pessoas e entidades, sejam essas relações jurídicas ou comerciais ou de caráter privado. Com isso, surgiram novas formas de obrigações nas relações, o que provocou uma verdadeira revolução tecnológica e social.

A busca de um melhor aproveitamento das oportunidades propiciadas pela rede mundial fez surgir a necessidade de constituição de um ambiente seguro para as relações digitais. Dentro desse quadro, a criação da autenticação eletrônica – agregando as facilidades das assinaturas digitais e dos serviços a elas associados, permitindo a autenticação informatizada dos dados – tornou-se um imperativo.

Como relatado anteriormente, as assinaturas digitais possibilitam ao destinatário de dados enviados eletronicamente, a verificação de autenticidade da origem e da integridade desses dados, através de tecnologias baseadas em um sistema criptográfico assimétrico, composto de um algoritmo (ou de uma série de algoritmos) que permite a geração de um par de chaves assimétricas exclusivas e interdependentes.

Para realizar a assinatura digital, tem-se recorrido ao emprego da criptografia, que possibilita a implementação e a utilização de senhas e chaves, o que proporciona um aumento significativo na segurança das comunicações virtuais. (Diniz,1999).

O aumento na quantidade de dados e informações estabelecidas à longa distância passou a exigir a utilização, em escala cada vez maior, de ferramentas de autenticação. Por isso, este capítulo tem como objetivo especificar uma modelagem da aplicação da assinatura digital em arquivos que precisam ser assinados digitalmente.

A modelagem escolhida, após efetivação da pesquisa, está fundamentada na utilização da Linguagem de Programação Java, uma vez que ela oferece, além de

facilidades na implementação, recursos adicionais relacionados à questão de segurança, como descritos a seguir.

3.1 A Linguagem Java

Segundo Campione & Walrath (1996), a linguagem Java é uma linguagem computacional completa, adequada para o desenvolvimento de aplicações baseadas na rede Internet e em redes fechadas. O lançamento da linguagem Java pela empresa norte-americana *Sun Microsystem*, na década de 1990, atraiu a atenção de programadores em todo o mundo devido às facilidades de programação, à robustez, ao gerenciamento de memória e à segurança que ela apresentava (Oaks, 1999).

Pelo fato de estar fortemente associada à Internet, um dos aspectos mais divulgados da linguagem Java é sua segurança. Segundo Schneier (200, p.170), “a linguagem Java é a única linguagem de programação projetada especialmente para o código móvel, e com a segurança em mente”.

Para Oaks (1999, p. 02), as diferentes expectativas em relação ao termo “segurança” trazem à pauta, quando se trata de programas implementados em linguagem Java, os seguintes itens:

- **Seguros contra programas maliciosos:** Programas não devem ter permissão para danificar o ambiente computacional de um usuário, incluindo cavalos de Tróia bem com programas nocivos que podem duplicar-se – vírus de computador.
- **Não-intrusos:** Deve-se evitar que os programas descubram informações privadas do computador *host* ou na rede de um computador *host*.
- **Autenticados:** A identidade das partes envolvidas no programa deve ser verificada.
- **Criptografados:** Os dados que o programa envia e recebe devem ser criptografados.
- **Examinados:** As operações potencialmente sensíveis devem sempre ser conectadas.
- **Bem-definidos:** Uma especificação de segurança bem-definida deve ser seguida.
- **Verificados:** As regras de operação devem ser definidas e verificadas.

- **Bem-comportados:** Deve-se evitar que os programas consumam muitos recursos do sistema.

3.1.1 Principais características da linguagem

Apesar de já ter sido amplamente promovida como linguagem para ambientes distribuídos complexos, como a rede Internet, a linguagem Java é de fato uma linguagem de computador de propósito geral que pode ser usada para escrever qualquer aplicação, desde simples programas de cinco linhas até aplicativos complexos, com recursos suficientes para a construção de uma variedade de aplicativos que podem ou não depender do uso de recursos de conectividade. (Garfinkel & Spafford,1999).

Entre as principais características que tornaram essa linguagem tão eficiente, estão a simplicidade, a eficiência e a familiaridade.

A simplicidade se deve ao número de construções da linguagem que são relativamente pequenos e, conseqüentemente, menos suscetíveis a erros de programação, tais como ponteiros e gerenciamento de memória, via código de programação. Por conter um conjunto de bibliotecas, a linguagem tem uma funcionalidade básica, que inclui rotinas de acesso à rede e criação de interface gráfica.

A linguagem Java pode ser se considerada eficiente, pois foi criada para uso em computadores pequenos, exigindo pouco espaço e pouca memória.

A familiaridade da linguagem se deve ao fato de compartilhar muitas características de linguagens comuns à maioria das linguagens de programação em uso na atualidade. Contudo, diferentemente da linguagem C e C++, a linguagem Java oferece gerenciamento automático de armazenamento e tratamento de exceções, integrado com suporte multilinha. (Arnold & Gosling, 1997).

Para manter a linguagem familiar, mas ao mesmo tempo pequena, os projetistas da linguagem Java removeram vários dos recursos disponíveis nas linguagens C e C++. Os recursos removidos foram principalmente aqueles que propiciam más práticas de programação, ou os que raramente são usados.

Outras características importantes da linguagem Java são: o “Paradigma da Orientação a Objetos”, o **“**Código Interpretado e Portável”, as “Aplicações distribuídas e processamento paralelo” e a “Segurança”.

- **Paradigma da orientação a objetos**

Isto significa que o programa, escrito em linguagem Java, é construído em função dos dados a serem manipulados e dos métodos que manipulam esses dados. Juntos, os dados e os métodos que os manipulam procuram simular o comportamento dos objetos do mundo real.

Arnold & Gosling (1997, p.1) relatam que: “os programas em Java são construídos a partir de classes. A partir de uma definição de classe é possível criar um número de objetos que são conhecidos como modelos daquela classe”.

Uma diferença básica entre a programação estruturada convencional e a programação orientada a objetos é algo chamado “*encapsulamento”*. O encapsulamento permite que se controle o acesso aos atributos e aos métodos que agem dentro de um objeto.

Para impedir o acesso aos dados (atributos) dentro de funções (métodos), na programação estruturada, basta tornar os dados de uma função disponível para outras funções. A maneira de fazer isto em um programa estruturado é tornar os dados globais em relação ao programa, o que fará com que qualquer tenha acesso a eles. Utilizando um outro nível de escopo – um que torne os dados globais às funções que precisassem deles – mas ainda impedir que outras funções ganhassem acesso. O encapsulamento faz exatamente isso. Num objeto, os membros dos dados encapsulados são globais em relação aos métodos dos objetos, mas não são locais em relação ao objeto, mas não são locais em relação ao objeto. Eles não são variáveis globais.

- **Código Interpretado e Portável**

A principal diferença entre uma linguagem compilada e uma linguagem interpretada refere-se ao tratamento do código.

Quando se utiliza uma linguagem compilada, é necessário executar um programa para traduzir os arquivos fonte, legíveis em linguagem de alto nível, em código

executável chamado de código binário. Esses aplicativos só podem rodar no tipo de computador para o qual foram compilados, uma vez que consistem, na realidade, em instruções em linguagem de máquina, entendidas e executadas pelo microprocessador.

As linguagens interpretadas só existem em código fonte. Quando um programa em linguagem interpretada entra em execução, um programa chamado interpretador toma o código fonte e executa as ações indicadas pelos comandos no arquivo. Desta forma o interpretador é o único aplicativo que está sendo executado.

A grande vantagem da utilização das linguagens interpretadas está no fato de que os programas podem ser implementados em uma variedade de plataformas diferentes, pois, como citado anteriormente, só existem em código fonte; isto também propicia maior facilidade de depuração.

Segundo Garfinkel & Spafford (1999, p. 41),

> os programas Java são compilados em um formato intermediário chamado bytecode independente de processador. Este bytecode é carregado na memória do computador pelo Carregador de Classe Java (Java Class Loader) e executado em uma Máquina Virtual Java (Java Virtual Machine – JVM).

A JVM (Java Virtual Machine) pode executar programas diretamente de um sistema operacional, como o Windows. Ou seja, um aplicativo Java pode rodar em qualquer sistema, desde que exista uma implementação da JVM para esse sistema. Por outro lado, pode ser embutida dentro de um navegador, permitindo que os programas possam ser executados à medida que estão sendo baixados da World Wide Web. Este é um aspecto bastante importante para aplicações distribuídas através da Internet ou de outras redes heterogêneas.(Oaks, 1999).

- **Aplicações distribuídas e processamento paralelo**

Pelo fato da linguagem Java ser adequada para uma gama extensa de aplicações que estejam dissociadas a Internet, a linguagem traz classes para o suporte a vários níveis de conectividade: acesso a URLs (padrão Internet), uso de conexões em sockets, criação de protocolos, criação de clientes e servidores. (Arnold & Gosling, 1997). A introdução desses conceitos, permitiu aos

programadores o acesso às informações da rede de forma simples, com a mesma facilidade encontrada no acesso aos arquivos locais.

Isso significa que bibliotecas de código nativo ou qualquer classe Java pode ser carregada em um interpretador Java a qualquer momento, mesmo quando ele já está rodando. Essas classes carregadas dinamicamente podem então ser instanciadas dinamicamente.

Para permitir uma melhor performance de execução, mesmo em tarefas de maior complexidade, a linguagem permite a programação de ***threads***, o que significa que um programa pode rodar vários processos paralelamente. (Knudsen, 1998). A linguagem traz também mecanismos para sincronização, ativação e desativação parametrizada desses processos.

- **Segurança**

Como citado anteriormente, a linguagem de programação Java foi projetada com a segurança em mente; por isso oferece várias camadas de controle de segurança que protegem contra códigos maliciosos, permitindo que os usuários rodem tranqüilamente programas de origem desconhecida, como os *applets* – que são programas executados por um browser da Web. (Knudsen, 1998).

Outra camada de proteção para segurança é comumente chamada de modelo de caixa de areia (sandbox): o código de origem desconhecida pode rodar, mas é mantido isolado dentro de uma caixa de areia, onde pode rodar em segurança sem causar qualquer dano ao "mundo real", que é o ambiente Java como um todo.

Segundo Schneier (2001, p.170) a caixa de areia é protegida por três mecanismos:

Verificador de código de bytes: sempre que um browser faz um download de um *applet* Java, o verificador de código analisa o código primeiro. O verificador garante que o código de bytes esteja formatado corretamente e não possua qualquer um dos vários problemas comuns.

Carregador de classe: esse componente determina como e quando um *applet* pode ser incluído no ambiente Java, certificando-se de que o *applet* não substituirá algo importante que já exista.

Gerenciador de segurança*:* é como um monitor de referência. Ele é consultado sempre que o *applet* Java tenta algo questionável, como abrir ou gravar um arquivo

ou abrir uma conexão na rede, entre outras. Dependendo de como o *applet* foi instalado, essas permissões serão permitidas ou negadas

3.1.2 O Pacote de Segurança Java

O Pacote de Segurança da linguagem Java (*package Java security*) é uma API complexa e pode ser relacionada a diversas implementações que permitem a criação de aplicações que utilizem recursos de segurança genéricos, como as assinaturas digitais.

Dois "*engine cryptography*" (motores de criptografia) padrões são encontrados neste pacote de segurança: um motor de compilação e mensagem e um motor das assinaturas digitais.

No pacote de segurança da linguagem Java, há um amplo conjunto de classes que funcionam nas chaves e que podem ser usados para gerar chaves secretas e pares de chaves (chave privada e chave pública).

As implementações concretas destas classes são fornecidas pela empresa *Sun Microsystem* no JDK (*Java Development Kit*), e só se tornaram possíveis através da infra-estrutura do provedor de segurança.

Segundo Oaks (1999, p.171):

> "Os provedores de segurança são a união que gerencia o mapeamento entre os motores usados pelo restante do pacote de segurança (como a compilação de mensagem), os algoritmos específicos que são válidos para tais motores (como uma compilação SHA) e as implementações específicas deste par algoritmo motor que pode estar disponível para qualquer máquina Java em particular."

Os provedores de segurança contam com a cooperação entre si mesmos e o resto dos pacotes de segurança Java para alcançar seu objetivo. Assim, torna-se responsabilidade da classe que está sendo usada perguntar à classe *Security* qual classe em particular será usada para executar determinada tarefa. A classe *Security*, por sua vez, pergunta a cada um dos provedores se pode ou não fornecer a compilação desejada. Portanto, um programa típico que deseja usar o pacote de segurança não interage diretamente com o provedor de segurança.

Para realizar uma determinada operação o pacote de segurança construirá uma *string*, representando-a, e pedirá à classe *Security* um objeto que possa realizar a operação com o algoritmo dado. É importante salientar que nem todo algoritmo pode ser usado para realizar toda operação; as combinações válidas são listadas no quadro abaixo:

Quadro 2 - Recursos de segurança e algoritmos esperados na API de segurança.

Motor (operações)	Nome do algoritmo
AlgorithmParameters *	DSA
AlgorithmParametersGenerator *	DSA
KeyFactory *	DSA
KeyPairGenerator	DSA
KeyPairGenerator	*RSA*
MessageDigest	MD5
MessageDigest	SHA-1
MessageDigest	*MD2*
Signature	DSA
Signature	*MD2/RSA*
Signature	*MD5/RSA*
Signature	*SHA-1/RSA*

Fonte: Oaks, Scott (1999, p.173)

As entradas em *itálico* e sublinhado do Quadro acima são operações que a especificação de segurança do Java define como legais, mas não são implementadas pelo provedor de segurança padrão.

A arquitetura que forma a base da API de segurança do Java, são baseadas nas classes *Security* e *Provider*, que, juntas, formam um conjunto de mapeamentos que permitem à API de segurança determinar dinamicamente o conjunto de classes que deve ser usado para implementar certas operações. (Knudsen, 1998).

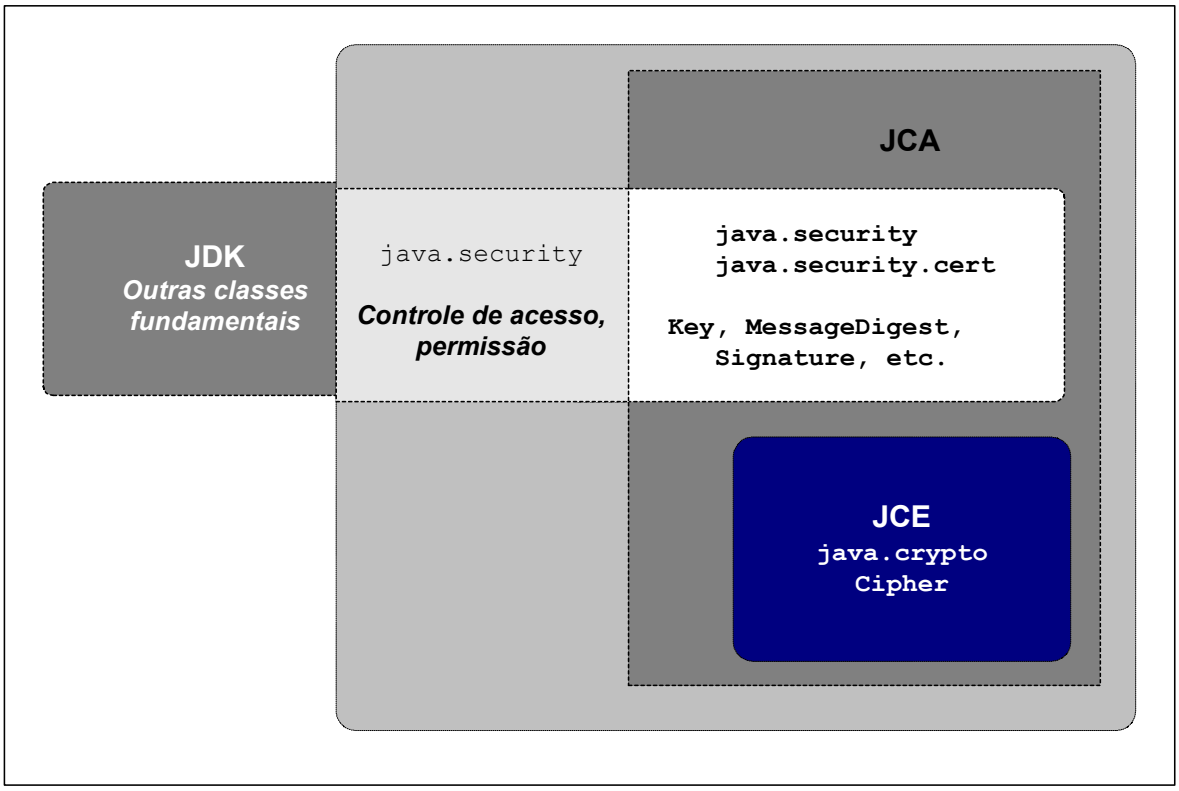

FIGURA 13 - Software API do Java Security.

Fonte: KNUDSEN, Jonathan (1998, p.30).

A figura 13, ilustra os vários grupos de Software API do Java Security. O JCA abrange as classes incluídas no JDK, bem como as extensões do JCE.

A seguir serão descritos os principais componentes do Java Security: a JCE (Java Cryptography Extension) e a JCA (Java Cryptography Architecture).

3.1.2.1 Arquitetura de Criptografia Java (JCA)

O projeto global da criptografia de classes é gerenciado pela Arquitetura de Criptografia Java (Java Cryptography Architecture – JCA). O JCA especifica o modelo padrão e uma extensa arquitetura para definir conceitos de criptografia e algoritmos. O JCA foi desenvolvido para separar conceitos de criptografia e implementações. Os conceitos são encapsulados por classes nos pacotes *java.security* e *javax.crypto*. As implementações são fornecidas pelos provedores de criptografia (*cryptographic providers*) da JCA (Knudsen, 1998).

A JCA foi projetada em torno dos seguintes princípios:

- Independência e interoperabilidade da implementação;
- Independência e extensão do algoritmo.

O conceito de independência das implementações específicas e independência do algoritmo permitem aos utilizadores da JCA usarem a API sem se preocuparem com as especificidades das suas várias implementações – concepção e implementação do algoritmo.

A independência da implementação é obtida através do conceito de "Cryptography Package Provider", que se refere a um "package" (pacote) ou um conjunto de pacotes que executam uma ou mais implementações de criptografia, sendo esses transparentes para a aplicação. Para cada *engine class* a utilizar, pode-se escolher qual o algoritmo criptográfico e/ou qual implementação desse algoritmo será utilizada, levando-se em consideração que a JCA normaliza a forma de nomear os diversos algoritmos criptográficos. Quando uma aplicação requisita um determinado algoritmo ao *framework*, este fornece uma implementação de qualquer um dos *providers* instalados.

A independência dos algoritmos possibilita a utilização de diversas técnicas criptográficas. Na linguagem Java, o motor de criptografia (*engine cryptographic*) funciona baseado no conceito de classes. Essas classes são chamadas de *engine classes* e implementam as diferentes funcionalidades dos algoritmos.

A possibilidade de extensão do algoritmo proporciona que novos algoritmos, com características diferentes dos existentes, sejam suportados pela JCA. Isto significa que novos *providers* podem ser acrescentados ao framework. Estes *providers* devem disponibilizar implementações das *engine classes* já especificadas.

A interoperabilidade de execução permite que implementações feitas por *providers* diferentes funcionem em conjunto. Um exemplo disso é o fato de que chaves geradas por um *provider* possam ser utilizadas para verificar uma assinatura digital, mesmo que esse algoritmo de verificação tenha sido implementado por um outro *provider*.

A JCA introduz o conceito de "Cryptography Package Provider": um pacote (ou conjunto de pacotes) que fornecem uma implementação concreta de um subconjunto dos serviços definidos na API.

Todos os *providers* implementam uma classe derivada da Classe Provider especificada no *packagejava.security*, dessa forma, o construtor desta classe

encarrega-se de registrar na JCA todas as implementações suportadas pelo pacote correspondente.

Isto permite à JCA reconhecer quais são os serviços e as implementações que estão disponíveis no sistema, e quais as bibliotecas a que pertencem, tornando possível instanciar os objetos correspondentes, quando necessário.

Das várias classes incluídas na JCA, serão listadas as mais importantes e que são base para a funcionalidade de uma assinatura digital.

- **Classe Engine**

Esta classe acompanha a Máquina Virtual Java e definem uma API para um serviço criptográfico independente do algoritmo e da implementação. Um serviço pode estar associado a operações como: efetuar operações criptográficas, como a assinatura digital ou o *hashing*; gerar material criptográfico (chaves ou parâmetros) necessário para efetuar operações criptográficas; gerar objetos de dados (repositórios de chaves - "keystores" ou certificados) que encapsulam chaves criptográficas de uma forma segura, dentre outras. (Arnold & Gosling, 1997).

- **Classe MessageDigest**

A classe MessageDigest pode gerar um valor de prova para qualquer entrada arbitrária e virtualiza o conceito criptográfico de função de *hash* (*digest*), que tem como entrada uma mensagem com dimensão variável (*array* de bytes) e como resultado uma mensagem de dimensão variável, que dependerá do algoritmo em uso.

- **Classe SecureRandon**

Esta classe é dedicada às operações de geração de números aleatórios ou pseudo-aleatórios (PRNG).

Segundo Knudsen (1998, p.293), “ao contrário do gerador de números aleatórios padrão, os números gerados por esta classe são criptograficamente seguros, ou seja, estão menos sujeitos à adivinhação do padrão e a outros ataques que podem ser feitos em um gerador de número aleatórios tradicional”.

- **Classe KeyPairGenerator**

A classe KeyPairGenerator é um dos *engines* padrões que podem ser fornecidos por um provedor de segurança Java, que irá gerar uma chave pública, bem como sua chave privada relacionada. As instâncias desta classe irão gerar pares de chaves apropriados para um algoritmo particular (DSA por exemplo).

- **Classe Signature**

A classe Signature é a classe, em linguagem Java, que representa as assinaturas criptografadas. Esta classe fornece a capacidade de criar e verificar as assinaturas digitais através da utilização de algoritmos diferentes que tenham sido registrados com a classe Security.

O objeto deve ser inicializado com a chave privada (para assinar) ou chave pública apropriada (para verificar). A assinatura então poderá ser gerada a partir dos dados inseridos no arquivo e depois verificada. O DSA/SHA-1 ou o RSA/MD5 são exemplos de algoritmos que realizam assinatura digital .

Apesar de ser muito semelhante à classe MessageDigest, a principal diferença entre elas é o fato de que, na classe Signature, uma chave terá que ser apresentada para funcionar em objeto de assinatura. Esta diferença é bastante importante, pois uma compilação de mensagem assinada não poderá ser alterada sem o conhecimento da chave que foi usada para criá-la. O mesmo não acontece em uma compilação de mensagem, onde a mesma pode ser alterada junto com os dados que ela representa, de tal forma que a adulteração seja imperceptível. (Oaks, 1999).

3.1.2.2 Extensão da Criptografia Java (JCE)

A Extensão de Criptografia Java (*Java Cryptography Extension* – JCE) baseia-se nos mesmos princípios da JCA: independência da implementação e, sempre que possível, a independência do algoritmo, utilizando a mesma arquitetura de *provider*.

O *provider* complementa o provedor padrão do JDK, e fornece estrutura para implementar a encriptação (simétrica, assimétrica e cifra de blocos), a geração e

distribuição de chaves e os algoritmos de Código de Autenticação de Mensagens (MAC).

Segundo Oaks(1999, p.278)

> ”A JCE segue a mesma infra-estrutura do provedor de segurança do restante da arquitetura de segurança de Java, é composta por um provedor de segurança adicional que inclui as implementações dos motores da JCE”.

A JCE era previamente um pacote opcional, que não podia ser obtido separadamente do JDK padrão (Java 2 SDK), versões 1.2.x e 1.3.x. No entanto, tem sido integrado na versão atual (Java 2 SDK, v 1.4), que incluem dois componentes de software (dados do fornecedor):

- Uma estrutura que define e suporta serviços para os quais os provedores podem fornecer implementação. Esta estrutura está toda incluída no pacote javax.crypto package.
- um provider nomeado "SunJCE"

O JCE 1.2 foi criado para estender a JCA a APIs disponíveis na plataforma de Java 2 e para incluir APIs e execuções para serviços criptográficos que ficaram sujeitos aos regulamentos de controle norte-americano de exportação, e estavam disponíveis apenas dentro dos Estados Unidos e Canadá.

Segundo Knudsen (1998), isto se deve a medidas de segurança quanto à codificação rigorosa que esta implementação é capaz de gerar. Tal restrição dizia respeito não somente ao uso, mas também à documentação eletrônica referentes a JCE.

Oaks (1999, p.278) relata que:

> “existem desafios legais contínuos para esta posição bem como um aumento das negociações com o governo americano para mudar esta política; ao mesmo tempo, há esforços crescentes para proibir o uso desta tecnologia mesmo nos Estados Unidos.”

Talvez em resposta a esses desafios, o JCE foi integrado no Java 2 SDK, v 1.4 e agora já pode ser exportado para outros países. Essa versão inclui habilidades de reforçar as limitações a respeito dos algoritmos de criptografia e a respeito das forças de criptografia máxima disponíveis para *applets*/aplicações em diferentes contextos de jurisdição. (Sun.M, 2002).

No entanto, ainda existem restrições quanto à importação da JCE no que diz respeito a versão da “criptografia forte” mais utilizada, principalmente nos países elegíveis (que são a maioria). Na França, por exemplo, é ilegal importar a JCE sem uma licença.(Oaks, 1999).

Desta forma, antes de utilizar todas os recursos de criptografia que a JCE dispõe (principalmente a “criptografia forte”), é recomendado verificar as políticas de segurança referentes ao país onde se dará tal utilização. De qualquer forma, a Sun Microsystem limita-se a oferecer suporte técnico e documentação eletrônica específica no que diz respeito a implementações de encriptação das APIs da JCE.

No que diz respeito à utilização da Extensão da Criptografia Java para as assinaturas digitais, Oaks (1999) descreve que as *engines cryptographic* (motores de criptografia) que fazem parte da JCE não são utilizados na geração e verificação das assinaturas digitais.

As assinaturas digitais utilizam algoritmos próprios para codificar e decodificar a compilação de mensagem. Assim, o motor de assinatura digital pode ser exportável, enquanto que os motores de criptografia não o são (Oaks, 1999).

Diversas empresas e grupos fora dos Estados Unidos implementaram novas APIs de segurança da JCE, desta forma existem diversos provedores de segurança de terceiros que incluem suas próprias implementações JCE e estão disponíveis fora dos Estados Unidos, incluindo o Brasil. As APIs que permitem calcular a compilação de mensagem e as assinaturas digitais são exportadas livremente.

3.2 Assinatura Digital e a Linguagem Java

Conforme citado anteriormente, a linguagem Java possui ferramentas adequadas que promovem o recurso indispensável à segurança no tráfego de dados em rede: a assinatura digital. Isto se deve ao suporte dado pela API Java à criptografia e ao tratamento de dados necessários à implementação das tecnologias que envolvem as assinaturas. Mesmo existindo algumas restrições à exportação de algumas ferramentas criptográficas, algoritmos de *hash* e chave pública-privada estão disponíveis; portanto, é possível criar um protocolo local para assinar documentos digitalmente.

O Pacote de Segurança do Java (*packetjava.security*) é o aspecto da linguagem Java mais importante para o desenvolvimento da assinatura digital, ao lado dos componentes JCA (*Java Cryptography Architecture*) e JCE (*Java Cryptography Extension*). Todo o suporte para a criptografia que será usada nesta modelagem está disponível em versões da linguagem a partir da versão 1.2 do JDK.

A figura 14, abaixo, dá uma visão geral da Modelagem do processo de assinatura proposta.

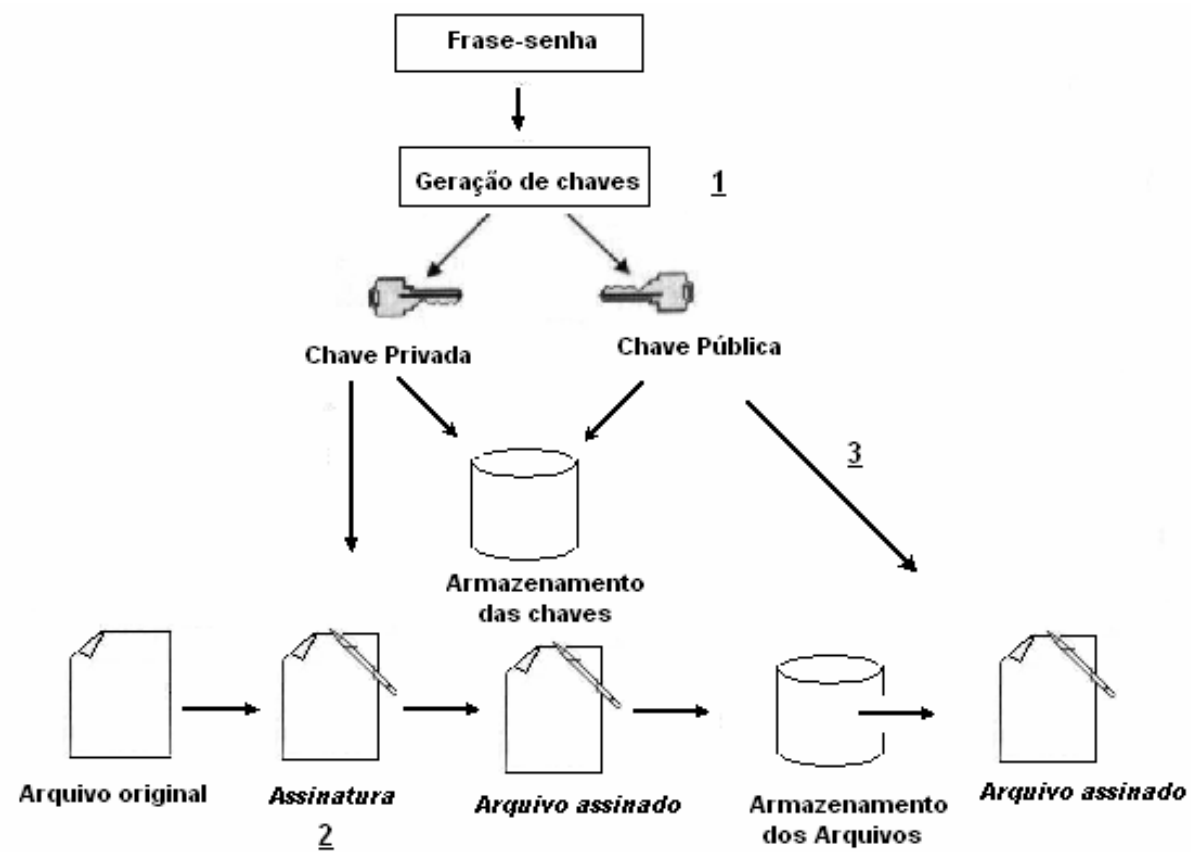

FIGURA 14 - Modelagem do processo de assinatura

Conforme ilustrada na figura 14, a modelagem do processo de assinatura proposta consiste na implementação dos seguintes passos: geração do par de chaves (privada e pública), geração da assinatura digital e verificação da assinatura.

Para todos os passos citados são requeridos algoritmos específicos de geração de chaves, resumos de mensagem e de assinatura, que são passíveis de utilização a partir da linguagem Java. O *package javax.crypto* e seus sub-pacotes (*subpackages*) são os responsáveis pela criptografia forte em Java e, dentro desses pacotes, é possível encontrar praticamente todas as ferramentas necessárias para implementar uma assinatura digital.

Dentre os algoritmos analisados na presente pesquisa, o que se mostrou mais adequado para modelagem da assinatura digital que tem sido buscada, foi o algoritmo DSA, tanto para gerar as chaves quanto a assinatura. Dentre outras características citadas anteriormente, o DSA oferece segurança em relação ao tamanho das chaves (1.024 bits), apresenta-se como um algoritmo padrão de assinatura, apresenta facilidades de implementação em Java e principalmente, é um algoritmo livre de patente, assim como o algoritmo de mensagem SHA-1.

A seguir serão descritos os procedimentos adotados em Java e os algoritmos utilizados na prática de uma assinatura digital.

- **Geração das chaves:**

O passo inicial na criação de uma assinatura digital é a geração de chaves, ilustrada na figura 15.

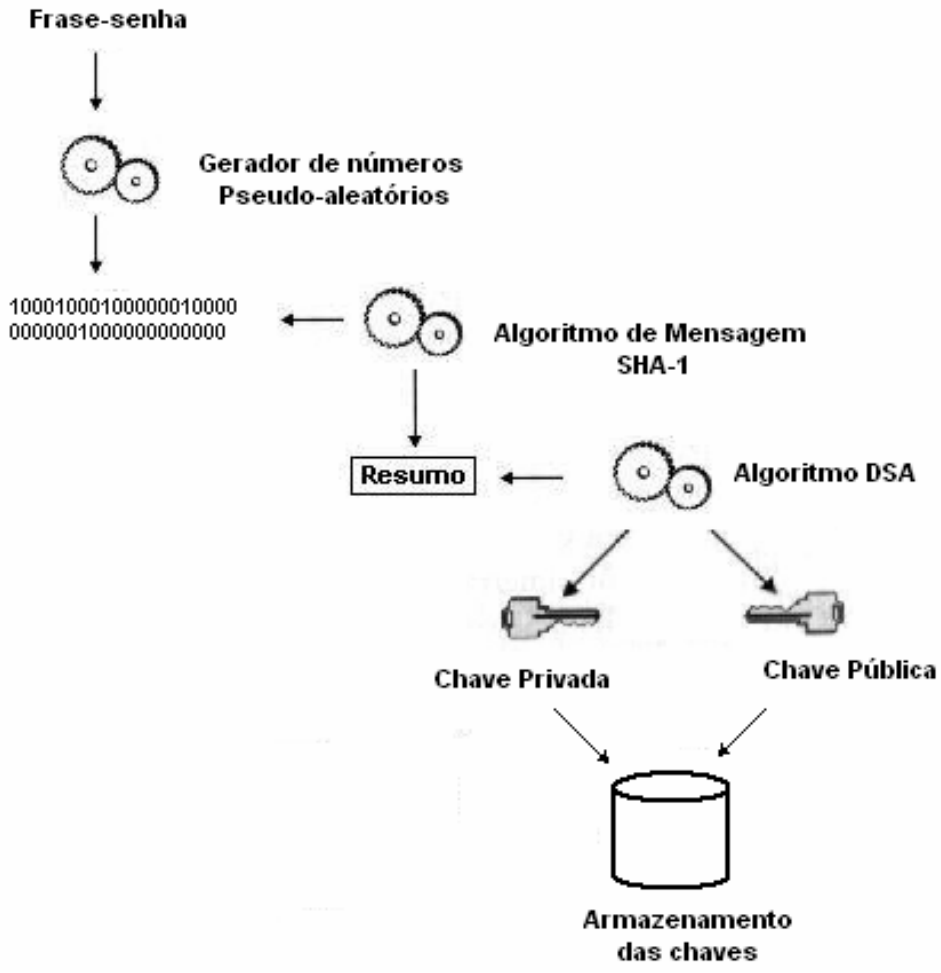

FIGURA 15 - Geração das chaves públicas e privadas.

A figura 15 demonstra o processo de geração do par de chaves assimétricas, que se inicia ao se informar uma “Frase-senha” ou “semente” (*seed*), que podendo ser uma seqüência tanto de números como de letras, que irá iniciar uma série.

Dada uma “semente” ou “Frase-senha”, será aplicado, sobre seus dados, um algoritmo de números “pseudo-aleatórios”, que efetivará o cálculo de um número a partir dos caracteres digitados, gerando uma série de números pseudo-aleatórios. A classe responsável por fornecer esses números pseudo-aleatórios é chamada de ***SecureRandom***. Ela gera números aleatórios que dificilmente se repetirão.

O algoritmo de mensagem SHA-1 aplicado à série obtida, resultará num resumo. A geração das chaves é possível através da classe ***KeyPairGenerator*** e do algoritmo DSA para gerar as chaves. O tamanho da chave deve ser compatível com o algoritmo sendo que, no caso do DSA utilizado, o tamanho pode variar de 512 a 1.024 bits.

O DSA aplicado ao resumo irá gerar duas chaves: uma privada e uma pública, que deverão ser armazenadas em arquivos separados (por questão de segurança). No JCE do Java existem objetos adequados para o armazenamento dessas chaves. O armazenamento da chave privada deverá ser feito, obrigatoriamente, de forma a mantê-la protegida.

- **Geração da assinatura digital:**

Após a geração do par de chaves, o processo de assinatura poderá ser realizado de acordo com o esquema ilustrado na figura 16.

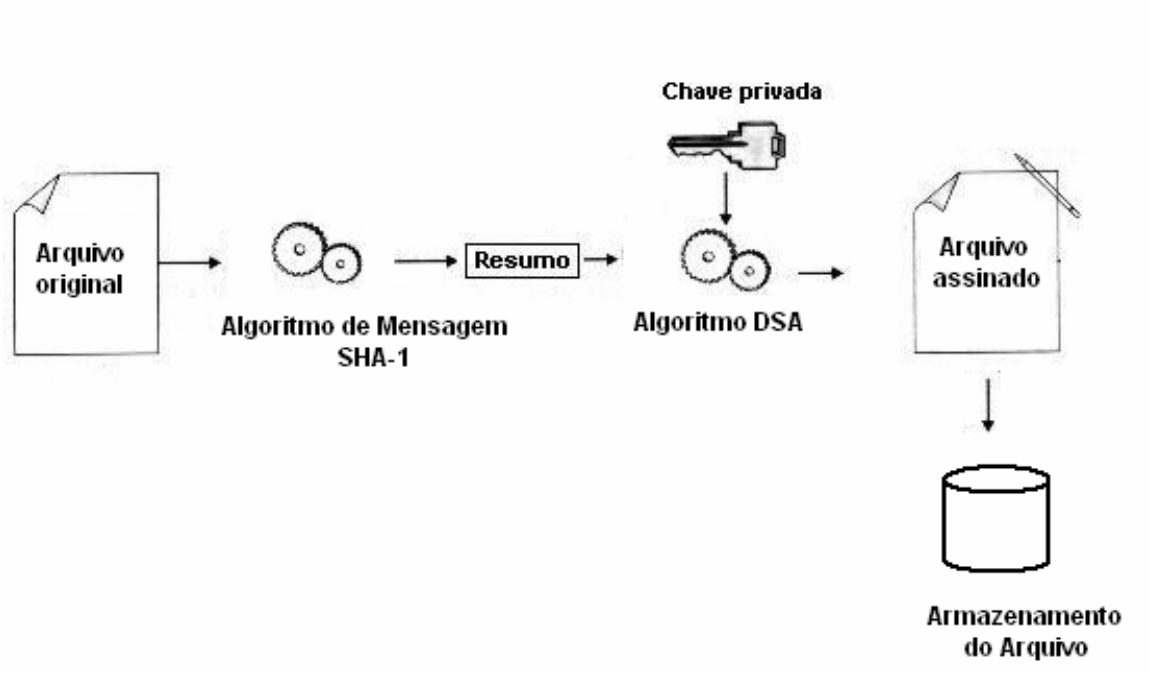

FIGURA 16 - Processo de assinatura

Esse processo é realizado para gerar a assinatura de um arquivo original e foi baseado nos algoritmos SHA-1 e DSA. É importante notar que tanto as chaves quanto a assinatura devem ser geradas utilizando-se o mesmo algoritmo de criptografia.

A classe responsável, no Java, por gerar as assinaturas digitais é chamada de ***Signature***. Com a posse da chave privada é possível dar início ao processo de assinatura propriamente dito, que consiste em, a partir de um arquivo original, aplicar-se o algoritmo de mensagem SHA-1 (que irá gerar um resumo) e o algoritmo de assinatura DSA (que iniciará a criação da assinatura digital); para tanto, utiliza-se a chave privada baseada nos dados inseridos no arquivo. O método usado para gerar a assinatura em Java é chamado de ***sign.***

Os dados gerados nesse processamento são, então, salvos e gravados, juntamente com o resumo que servirá como assinatura; desta forma, tanto os dados quanto a assinatura poderão ser recuperados em uma data posterior. Qualquer alteração realizada em um arquivo assinado implicará no início do processo de assinatura.

Aqui terminam as responsabilidades do assinante. Tudo o que ele precisa fazer agora é fornecer a chave pública juntamente com o dado a ser enviado e a assinatura correspondente.

- **Verificação da assinatura digital:**

Tendo acesso à chave pública e à assinatura digital, que são enviadas juntamente com os dados, é possível validar tanto os dados quanto a assinatura. A figura 17 ilustra de que forma é feita esta validação.

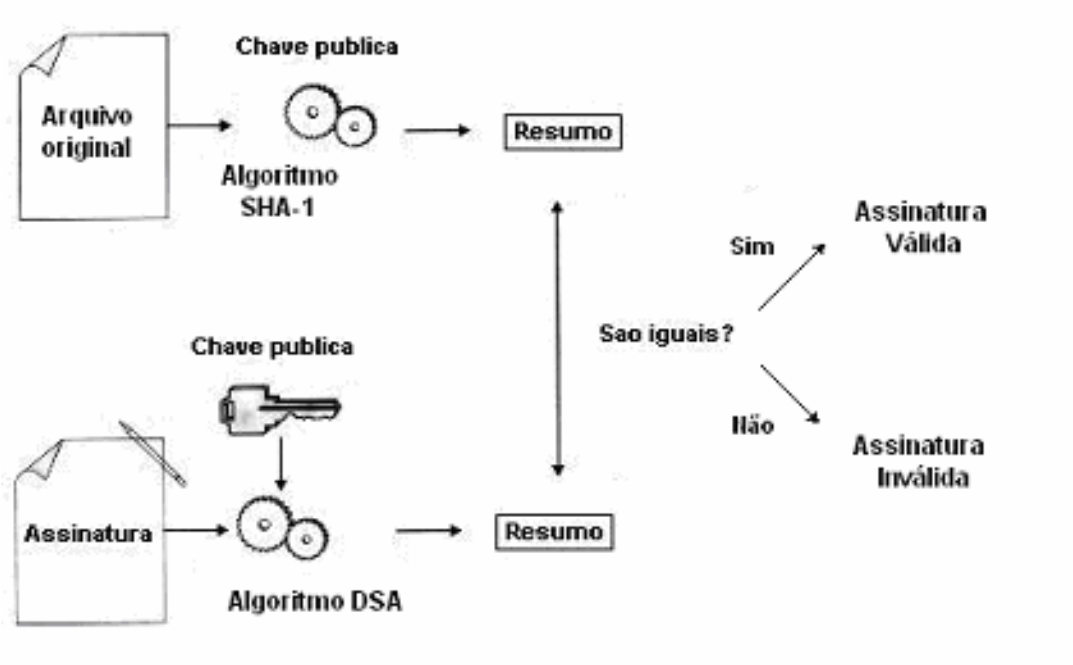

FIGURA 17 – Processo de verificação da assinatura

Como mostra a figura 17, o processo de verificação da assinatura digital, realizado a partir dos dados e da assinatura, utiliza tanto a chave pública (correspondente à chave privada que a gerou) quanto os algoritmos SHA-1e DSA.

Após a abertura do arquivo original, aplica-se o algoritmo de mensagem SHA-1 no resumo (o qual foi enviado juntamente com o arquivo) e, para verificação da integridade da mensagem, utiliza-se a chave pública e o algoritmo DSA sobre a assinatura, sendo que ambos produzirão resumos que serão comparados. O método usado para se fazer verificação da assinatura é denominado ***verify*.**

Se as respostas dos resumos forem iguais, a assinatura será confirmada.

Os programas-fonte, em Java, criados para gerar chaves, registrar e verificar a assinatura digital encontram-se em anexo no final desta dissertação (Anexo 1).

4 UTILIZAÇÃO DOS RECURSOS DE ASSINATURA DIGITAL NO SISTEMA DE INFORMATIZAÇÃO PROCESSUAL

Este capítulo tem como objetivo apresentar um modelo computacional para o trâmite de processos e documentos em uma repartição pública, levando-se em consideração a parceria estabelecida entre o Departamento de Expressão Gráfica, da Universidade Federal de Santa Catarina, e o Tribunal Regional do Trabalho, da 14ª Região – Rondônia e Acre, na sistematização do acompanhamento processual em todas as suas fases e etapas. Este acompanhamento será feito mediante a utilização das tecnologias que envolvem a assinatura digital e a modelagem de implementação proposta em Java.

O modelo proposto foi baseado no acompanhamento das funcionalidades do sistema atual, na disponibilidade de recursos físicos e monetários, na pesquisa das tecnologias inerentes à assinatura digital e na viabilidade de integração dessa técnica no aperfeiçoamento da segurança do Sistema de Informatização Processual.

4.1 Descrição do Sistema de Informatização Processual

O aplicativo atualmente em uso na Primeira Instância da Justiça Trabalhista é denominado Sistema de Informatização Processual (SIP) e tem por objetivo a realização de tarefas jurisdicionais, a melhoria das condições de trabalho dos serventuários da justiça e a agilidade dos serviços prestados a comunidade. O sistema tem por base uma filosofia de integração total, possibilitando, assim, que os dados sejam alimentados somente uma vez e posteriormente estejam disponíveis a todos os usuários, de acordo com critérios pré-estabelecidos.

O SIP é um aplicativo que tem como tarefa principal não somente o acompanhamento processual em primeira instância, no Poder Judiciário, mas também o auxílio para consultas a esses processos que podem envolver: cálculo de custas, controle estatístico, emissão de relatórios diversos, entre outros. Sua característica básica é a informatização de todas as fases da ritualística processual, que se inicia com o cadastramento de todos os dados correspondentes ao processo, e continua com o acompanhamento da distribuição, da autuação, do

acompanhamento junto às Varas e Cartórios, do registro e controle de audiências, dentre outros. Todo esse processo fornece apoio para a elaboração de sentenças e despachos e facilidades para emissão e gerenciamento de documentos (certidões, mandados judiciais, despachos, editais, atas, outros expedientes e publicações legais, cálculos, registros e controles de guias de custas, consultas diversas).

O Sistema é formado por uma base de dados única que servirá para utilização nos processo de Segunda instância, havendo, portanto um reaproveitamento de informações básicas e evitando a duplicidade das mesmas.

Dentre as principais características que o sistema propiciou à Justiça do Trabalho, estão listadas abaixo as facilidades e o seu ambiente de trabalho.

Principais facilidades criadas pelo SIP:

- Os dados são armazenados em um único banco de dados, o que permite sua recuperação e cruzamento para elaboração de estatísticas e prestação de informações ao público de forma extremamente facilitada, respeitando sempre os critérios de segurança de acesso às informações;
- Cadastro separado para acesso distinto de partes e de advogados;
- Eliminação de livros de carga de processos, através do encaminhamento eletrônico e/ou guias emitidas pelo sistema;
- Pesquisa de processos através da combinação de informações;
- Emissão de certidões;
- Pesquisa de nomes por semelhança fonética;
- Controle de prazos e de execução de tarefas.

Ambiente:

- **Arquitetura Cliente/Servidor:** O SIP é um sistema que possui uma interface que trabalha em conjunto com os principais gerenciadores de banco de dados existentes no mercado.
- **Ambiente Multi-usuário:** A base de dados do sistema pode ser consultada e atualizada por múltiplos usuários simultaneamente, sendo a segurança e a integridade das informações armazenadas garantidas pelo SIP/PI.

- **Integração das Informações:** O SIP é um sistema desenvolvido em ambiente de Banco de Dados, dentro de uma filosofia de processamento integrado, onde uma informação é digitada uma única vez e fica disponível para qualquer módulo que precise fazer uso da mesma.
- **Segurança:** Agregado ao SIP, existe um Módulo de Segurança, pelo qual o Administrador do Sistema autoriza ou proíbe o acesso de usuários a funções ou informações específicas. Este módulo também é responsável pela auditoria no Sistema.
- **Impressão:** Todos os relatórios podem ser visualizados na tela ou impressos em qualquer impressora disponível no Sistema Operacional;
- **Linguagem empregada:** A implementação do SIP foi desenvolvida utilizando a Linguagem de Programação Java. Esta é uma característica importante, no que se refere ao ambiente, em virtude das vantagens do Java, já citadas.

4.1.1 Composição do Sistema

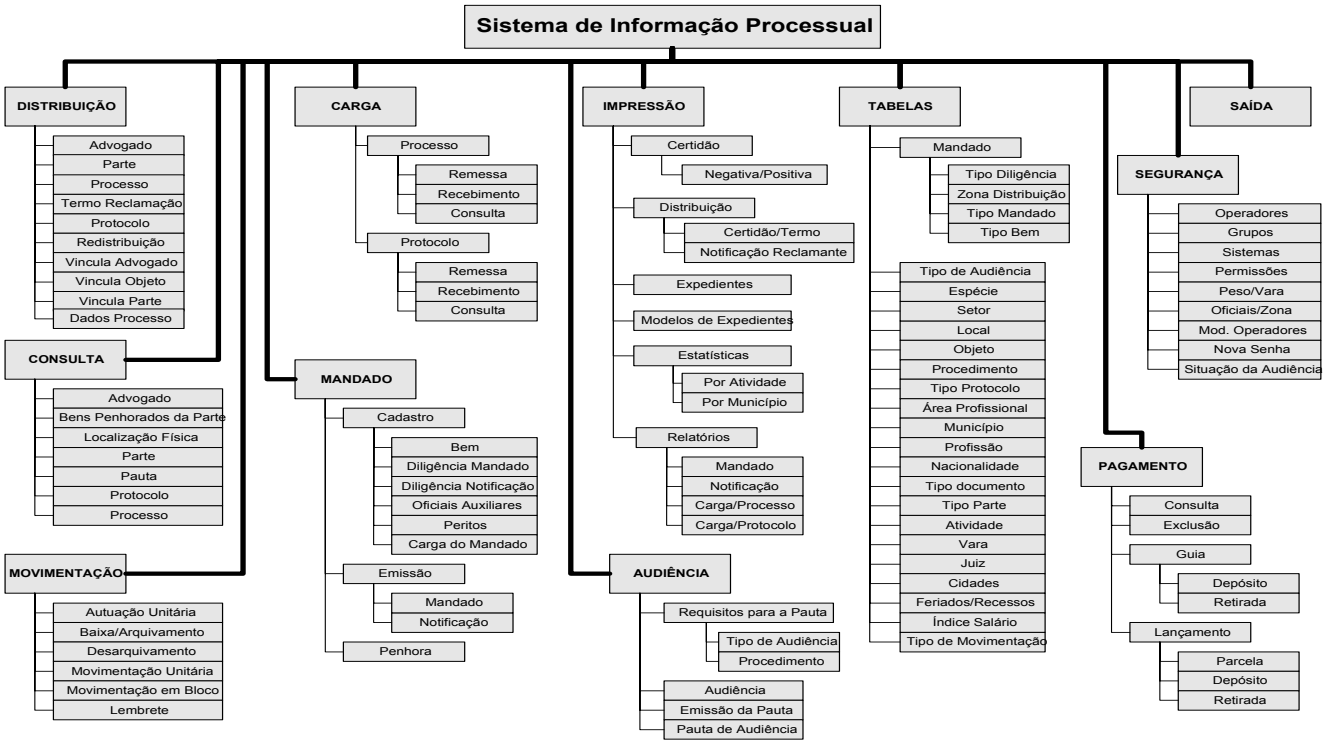

FIGURA 18 – Módulos do SIP

Conforme ilustrado na figura 18, o sistema é composto por dez módulos que integram as funcionalidades do sistema, a saber:

- **Módulo de Distribuição:** tem por objetivo realizar o cadastro dos processos judiciais, bem como das diversas partes envolvidas nesse processo, além de registrar a vinculação das partes do processo, os advogados de cada parte do processo, a distribuição e redistribuição de processos por sorteios;
- **Módulo de Consulta:** propicia a realização de consultas a processos cadastrados, seus advogados e partes, assim como a: pautas de audiência, bens penhorados de partes, e a localização física de processos e protocolos;
- **Módulo de Movimentação Processual:** tem por objetivo realizar a movimentação unitária de processos, a movimentação de vários processos de forma simultânea, a baixa e a reativação de processos, a localização física de processos, assim como o controle da pauta de audiências;
- **Módulo de Carga:** visa realizar o controle de remessa, recebimento e consulta dos processos e mandados, possibilitando a eliminação dos livros de carga. Este controle se torna mais efetivo tanto no que diz respeito aos prazos de devolução, quanto às localizações;
- **Módulo de Mandados:** tem por objetivo permitir a realização da emissão e controle de qualquer mandado/notificação utilizado no dia-a-dia do Cartório ou Vara e também permite a utilização da Central de Mandados, Controle e Distribuição de Mandados/Notificação por Oficial de Justiça, além do Controle de Diligências, Emissão de Relatórios Diversos, Vinculação e Controle de Penhoras;
- **Módulo de Audiência:** visa permitir o suporte para os procedimentos de marcação de Pauta de Audiências e geração do “Termo de Audiência”, ou “Ata de Audiência”;
- **Módulo de Pagamento:** tem por objetivo permitir a definição dos tipos de recolhimentos por tipo de custas, como também a definição das regras de cálculo para cada tipo de recolhimento. Além disso, efetua o cálculo das custas para um processo conforme os recolhimentos e regras pré-estabelecidos, realiza a atualização monetária dos valores históricos, efetua o

cálculo de honorários de advogados e emiti a conta de custas e guias de recolhimento;

- **Módulo de Impressão:** visa realizar a impressão de certidões, dados processuais, estatísticas por cartório, por comarca, por magistrado, por classe de processos e por tipo de movimentação, além de permitir que novas formas sejam definidas;
- **Módulo de Tabelas:** tem por objetivo realizar o cadastramento, alteração, consulta e exclusão de todas as tabelas básicas, visando o perfeito funcionamento do sistema;
- **Módulo de Segurança:** visa realizar o cadastramento dos usuários do sistema e respectiva lotação assim como a liberação da autorização para acesso e atualização do banco de dados automaticamente. Este módulo será visto com mais detalhes a seguir.

4.2 Utilização das tecnologias da assinatura digital no Sistema de Informatização Processual

O aperfeiçoamento da segurança do Sistema de Informatização Processual (SIP), será realizado acrescentando ao Módulo de Segurança a tecnologia da assinatura digital e as facilidades dos serviços associados a ela, permitindo a autenticação informatizada dos documentos (processos, mandatos, certidões, entre outras), o que irá garantir a autenticidade e a integridade dos mesmos.

A utilização da assinatura, no SIP, contará com os mecanismos de autorização e permissão que estão diretamente relacionados às propriedades de controle de acesso e disponibilidade de serviços, já implementadas no sistema atual.

A figura 19, abaixo, dá uma visão geral do funcionamento da assinatura digital integrado ao Módulo de Segurança do SIP.

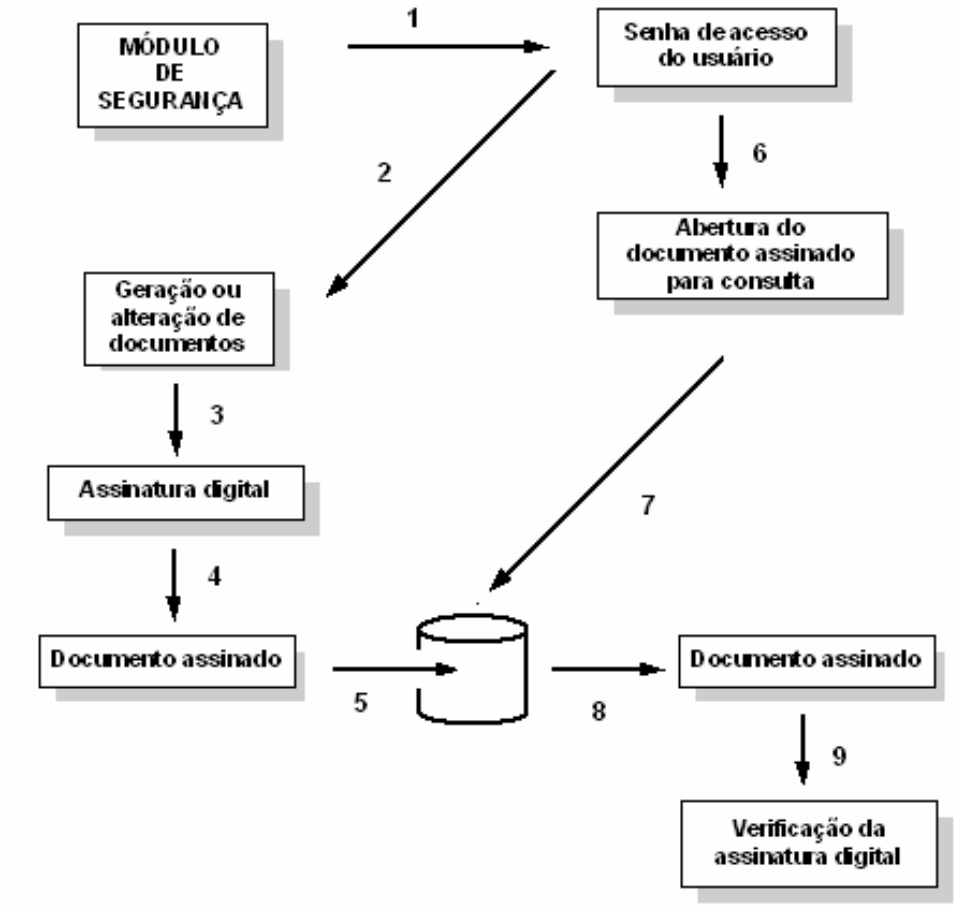

FIGURA 19- Funcionamento da assinatura digital integrado ao SIP.

Conforme pode ser visualizado na figura acima, o Módulo de Segurança faz o cadastramento dos usuários e restringe o acesso aos recursos disponíveis no SIP. Toda e qualquer assinatura autorizada é inserida em um documento antes de ser armazenado, e, no momento da consulta (por usuários autorizados), é realizada a verificação dessa assinatura.

Atualmente o acesso aos recursos do sistema pelos usuários é realizado através da inserção de um nome do usuário e senha, conforme ilustrado abaixo (figura 20).

FIGURA 20 -Visualização da tela de abertura do sistema

Essa figura reproduz a tela inicial do sistema SIP. Para utilização do sistema, os usuários deverão preencher os campos nome e senha, pré-cadastrados no Módulo de Segurança. Após a verificação de integridade dos dados inseridos, surge a tela principal do sistema (conforme figura 21, abaixo), que possibilita a navegação pelos módulos que compõem o SIP, já descritos.

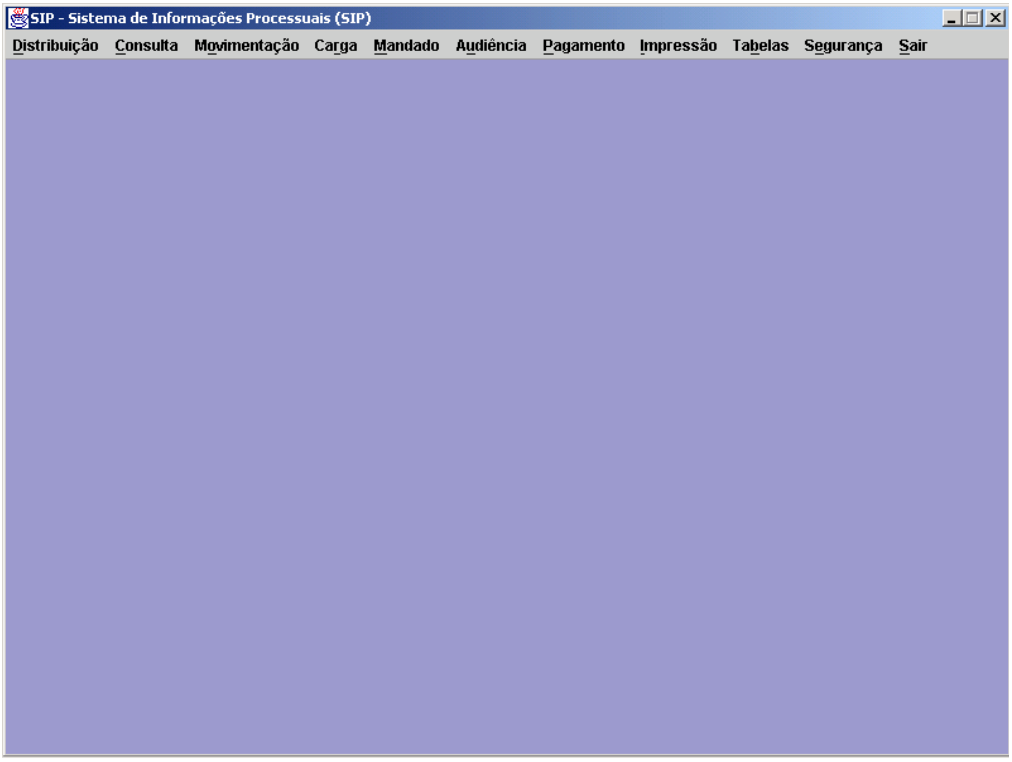

FIGURA 21 - Tela principal do sistema

Como mencionado, é no Módulo de Segurança do SIP que o operador do sistema irá cadastrar o usuário e sua senha de acesso e definir em que grupo e categoria o mesmo será cadastrado. Após essa definição, será feita a liberação ou restrição para cada tela do sistema e, em cada tela, funções específicas; a liberação de autorização para acesso e atualização do banco de dados, consultas e relatórios

de auditoria. Todas as operações atualizadas do banco de dados podem ser identificadas pelo usuário e pela data e hora em que foram realizadas.

Com base nos cadastros dos usuários e suas prioridades de acesso, a assinatura digital será inserida em todo e qualquer trâmite processual criado ou alterado e, só após essa inserção, as alterações serão armazenadas no banco de dados, para consultas posteriores.

Para assinar digitalmente um documento, os usuários autorizados deverão obrigatoriamente gerar um par de chaves assimétricas, sendo uma privada (que deverá estar seguramente protegida) e outra pública (disponível). O processo de geração de chaves pelo usuário, será tratado da mesma forma que as senhas de acesso ao sistema.

O operador do sistema irá gerar um código e uma senha para o usuário. Após o recebimento, o mesmo deverá fazer a alteração da frase-senha disponível no menu principal do SIP acessando o módulo de segurança.

A figura abaixo ilustra a tela que o usuário utilizará para fazer a alteração da frase-senha, sendo que, quando do ingresso no sistema, o usuário deverá digitar, no campo Frase-senha, a senha informada pelo operador do sistema e, nos campos Nova Frase-senha, o usuário deverá digitar a nova senha de chave e confirmá-la no campo seguinte. A nova Frase-senha pode ser composta por caracteres ou números.

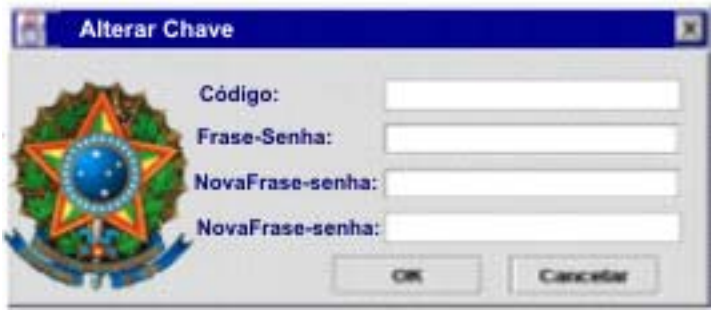

FIGURA 22 - Alterar Chave do usuário

As chaves geradas ficarão armazenadas no banco de dados na tabela denominada “TABELA DE CHAVES”, que irá conter os seguintes campos: Código do Operador, Descrição da Chave Pública, Descrição da Chave Privada, Data e Hora da Chave e a Data e Hora de Revogação.

O campo Código do Operador aparecerá nesta tabela para que possa ser relacionado com a tabela do Operador do sistema, que conforme já descrito, será

responsável pelo cadastro do usuário e a emissão do par de chaves. Os campos Descrição da Chave Privada e Descrição da Chave Pública também se encontram na tabela por estarem diretamente relacionadas com o processo de assinatura, sendo a primeira utilizada para assinar um documento e a segunda utilizada para se proceder à verificação.

A permanência da chave privada no banco de dados se faz conveniente para que o usuário não precise informar a “frase-senha” todas as vezes que criar ou alterar um documento.

O campo Data e Hora da Chave refere-se à data e à hora de criação do par de chaves e o campo Data e Hora de Revogação identifica a data e a hora que o par de chaves perdeu a validade. Os dois campos baseiam-se na data/hora do banco de dados do sistema.

É importante salientar que a Data e Hora de Revogação são empregadas caso haja a necessidade de se anular um par de chaves existente, desta forma todos os documentos assinados antes da revogação das chaves, poderão ser visualizados respeitando a data e a hora existentes nesse campo.

Em todos os módulos existentes no sistema, onde haja um editor de texto disponível e que seja possível criar ou alterar um documento, existirá um processo de assinatura, conforme ilustrado na figura 23.

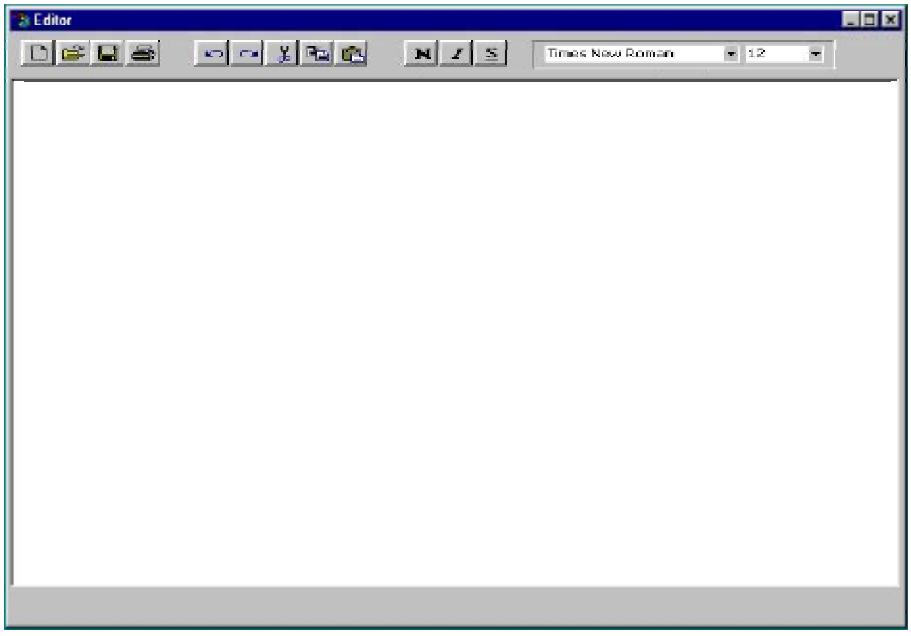

FIGURA 23 - Editor de texto do Cadastro e Distribuição de Processos do Módulo de Distribuição do SIP

O editor de texto mostrado na figura 23 localiza-se no Módulo de Distribuição do SIP, o que faz com todos os dados do documento sejam assinados digitalmente.

Após o término da criação ou alteração de um documento, o usuário irá salvá-lo na Tabela de Documentos. O processo de assinatura do arquivo, acontecerá no momento da sua gravação, quando será disparado um *procedimento* pelo banco de dados utilizando um programa de inserção da assinatura digital implementado em Java, conforme proposto no Capítulo 3.

A impossibilidade de inclusão do documento na Tabela de documentos, implicará na aparição da caixa de diálogo reproduzida abaixo.

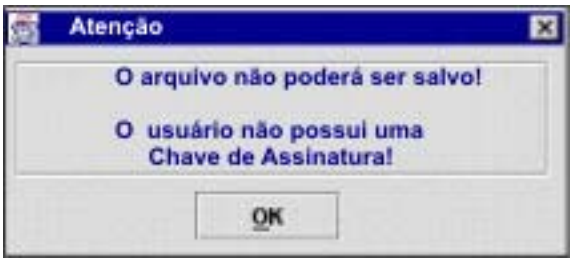

FIGURA 24 - Caixa de Diálogo do Editor de Texto.

Conforme ilustrado na figura 24, o usuário que não possuir uma chave privada válida não poderá gravar arquivos no banco de dados. A validade da chave privada pode estar relacionada com a sua revogação, ausência ou problemas no cadastro da mesma no Módulo de Segurança.

A verificação da assinatura digital inserida nos documentos gravados no banco de dados do SIP, será realizada no Módulo de Consulta. A seguir será mostrado o procedimento que o usuário irá realizar para a consulta de um processo assinado.

A tela reproduzida na figura 25, abaixo, propicia efetivar consultas a dados referentes a Processos Judiciais.

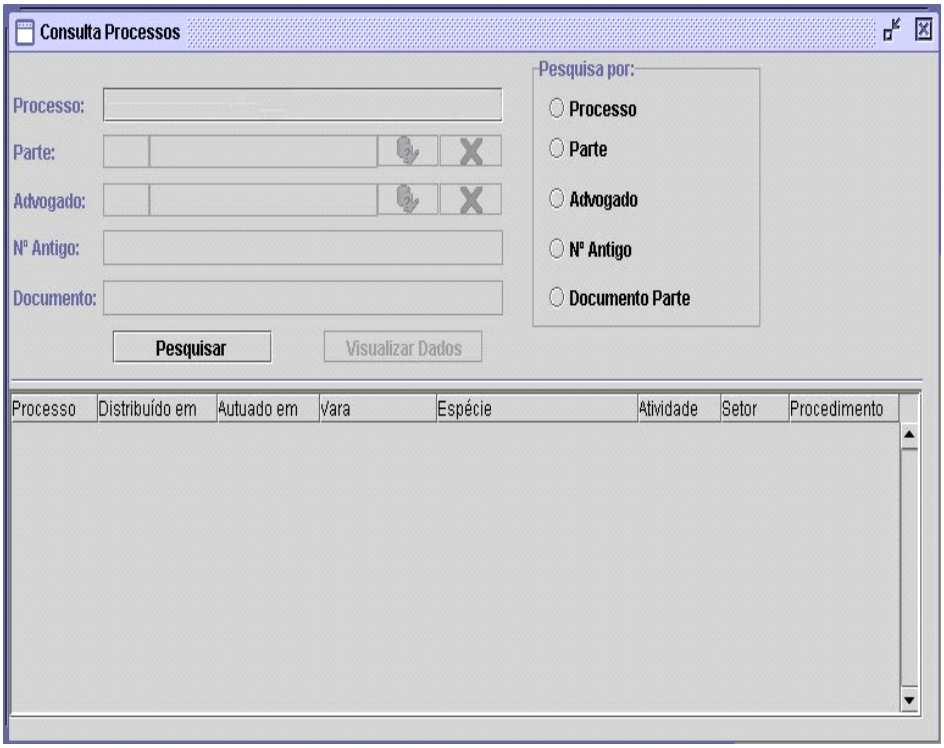

FIGURA 25- Consulta de Processos

Ao utilizar essa tela, o usuário irá selecionar uma das opções de consulta referentes ao Processo. A pesquisa pode ser feita por Processo, Parte, Advogado, Número Antigo ou Documento Parte.

Caso a opção selecionada tenha sido “Consulta por Processo”, no campo Processo deverá ser preenchido o Número do Processo a ser pesquisado. O sistema disponibilizará os resultados da pesquisa na forma de tabela, conforme deixa ver a figura acima (figura 25).

Para visualizar os dados de um Processo, o usuário irá selecioná-lo e irá clicar no botão “Visualizar Dados”. O resultado será disponibilizado na tela “Visualiza Dados do Processo” , conforme figura 26, abaixo.

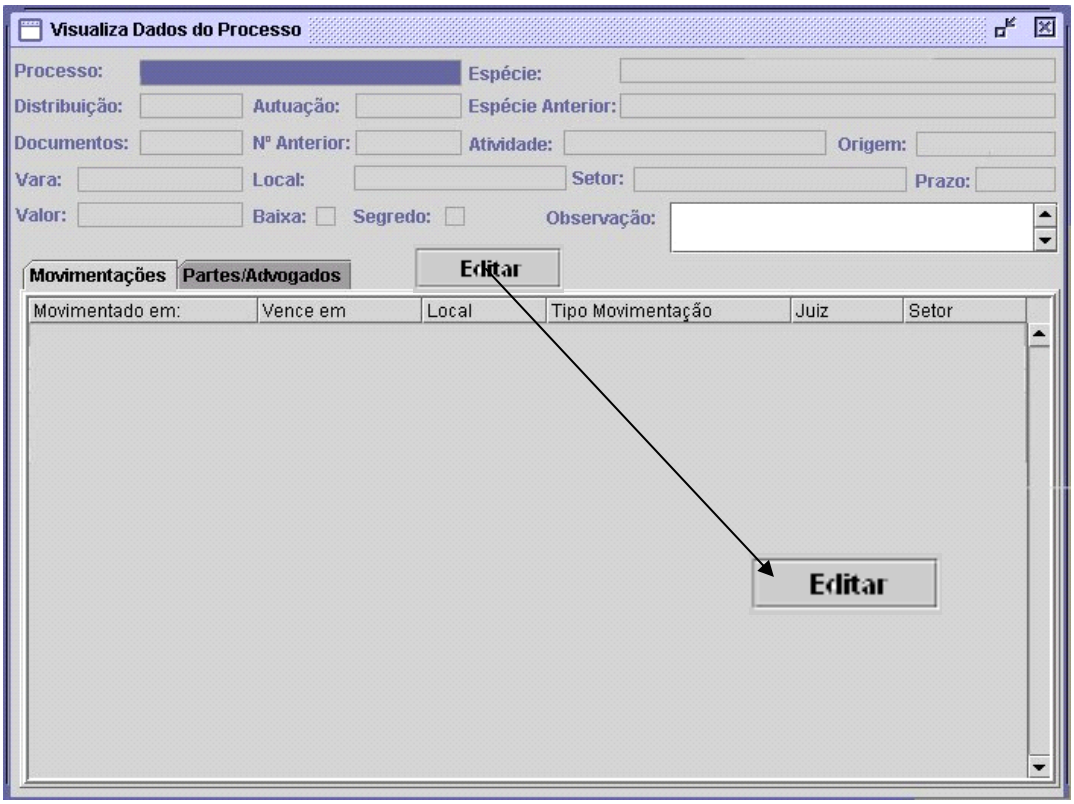

FIGURA 26 – Visualiza Dados do Processo

Essa tela mostrará todos os dados referentes ao Processo consultado. Se o botão “Editar” for clicado, será gerado um texto a partir dos dados mostrados nos campos. Todo Processo será visualizado no editor de texto, que também propiciará a verificação da assinatura digital, como mostrado na figura abaixo.

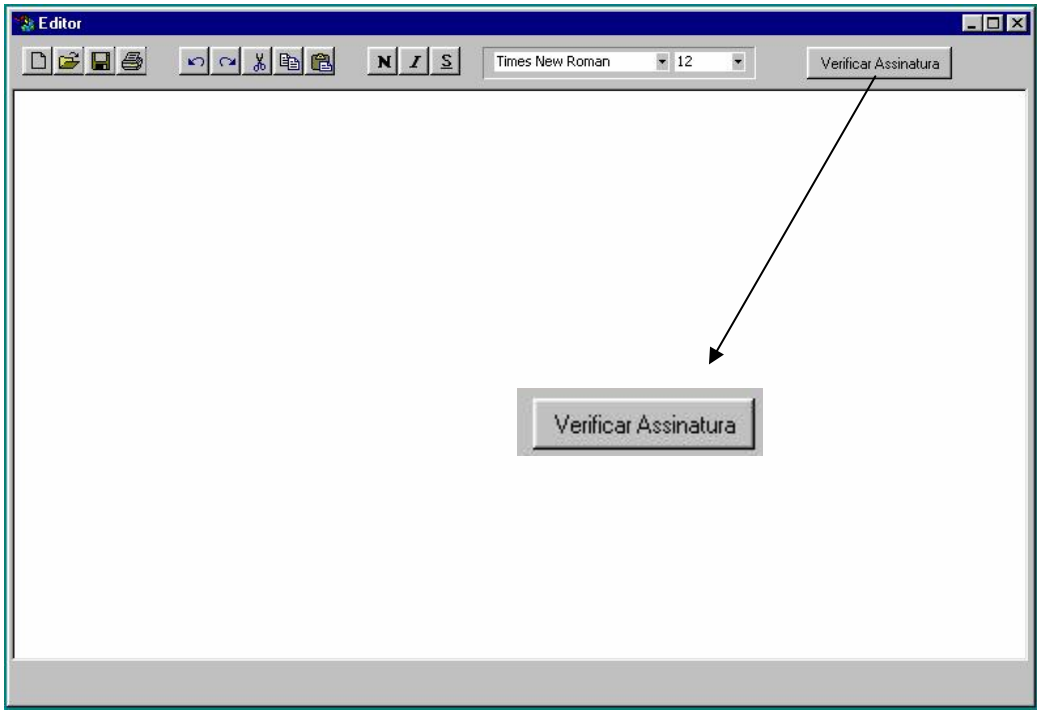

FIGURA 27 - Editor de texto (verificação da assinatura).

A figura 27 ilustra a tela em que o Processo será editado e a verificação da assinatura digital será feita, atestando o conteúdo do documento e a identidade do assinante. A verificação será realizada utilizando o programa de verificação da assinatura digital implementado em Java, conforme proposto no Capítulo 3.

A tela abaixo (figura 28) será mostrada caso a assinatura seja validada.

FIGURA 28 - Caixa de Diálogo mostrada na Verificação da Assinatura.

A figura 28 ilustra como o sistema atesta a validade da assinatura digital inserida no documento, desta forma o usuário poderá confiar na autenticidade do documento e na identidade do assinante, caso contrário, será indicada a Caixa de Diálogo abaixo (figura 29).

FIGURA 29 – Caixa de Diálogo mostrada na Verificação da Assinatura.

A tela ilustrada na figura 29 indicará que ocorreram problemas na verificação da assinatura, desta forma o usuário não poderá ter certeza se a assinatura inserida é realmente de quem diz ter assinado ou se os dados contidos no documento foram alterados indevidamente.

5 CONCLUSÃO

Neste trabalho foram abordadas as propriedades de Autenticação e Integridade que, segundo Wadlow (2000), são alguns dos princípios de segurança que levam ao que se pode entender como um sistema seguro. Essa duas propriedades podem ser obtidas com a implementação das assinaturas digitais (Schneier, 2001).

Partindo desses princípios e dos estudos realizados ao longo deste trabalho, foi possível propor um modelo de integração da técnica da assinatura digital ao Sistema de Informatização Processual (SIP), tomando como base as propriedades de segurança já existentes no sistema atual (Controle de Acesso e Disponibilidade de Serviços).

O modelo proposto pode agregar valor ao sistema atual, sem diminuir sua funcionalidade, levando-se em consideração que o modelo proposto:

- Seguiu o padrão de interface do sistema atual.
- Utilizou, na modelagem de implementação da assinatura digital, a mesma linguagem escolhida pela equipe de desenvolvimento do SIP, facilitando assim o trabalho de implementação dos mesmos. Isto se deve ao conhecimento prévio das rotinas do sistema, comandos e funcionalidades da linguagem Java.
- Utiliza, na modelagem da assinatura digital, algoritmos que são considerados seguros, apresentam facilidades de implementação em Java e são livres de patente.
- A interface gráfica não sofrerá mudanças que poderia vir a comprometer a utilização do sistema por parte dos usuários.
- A integração do processo de assinatura ao Módulo de Segurança será tratada da mesma forma que as senhas dos usuários utilizadas atualmente.
- A assinatura inserida nos documentos criados no SIP não terá questionada sua validade jurídica.
- O processo de assinar um documento será realizado apenas pelos usuários internos do sistema.

Como a interface do SIP não sofrerá grandes alterações após a implantação da assinatura digital, não haverá necessidade de todos os usuários passarem por novos treinamentos para utilizar este novo recurso de segurança. Somente os

usuários que possuem autorização para gravar novos documentos no Banco de Dados, terão que ser notificados da necessidade de criar uma chave de assinatura.

Desta forma, com a integração do processo de assinatura digital ao Módulo de Segurança, os usuários do Sistema de Informatização Processual (SIP) poderão contar com mais um recurso de segurança – as assinaturas digitais – que possibilitará a autenticação informatizada de todos e quaisquer trâmites processuais. Assim, o sistema (SIP) como um todo realizará mais tarefas, o que lhe agrega valor, e terá sua confiabilidade incrementada, o que o coloca na classe dos sistemas adaptados às novas necessidades que a própria dinâmica dos tempos de Internet impõem.

5.1 Recomendações para trabalhos futuros

A tecnologia digital tem uma série infinita de inovações, conseqüências não desejadas e surpresas, e não há motivos para acreditar que isso logo terminará. A Segurança é um processo e não um produto e os sistemas digitais se tornarão cada vez mais complicados. Schneier (2001).

As tecnologias digitais vêm sendo aplicadas aos mais diversos produtos (softwares comercias, jogos, telefones celulares, carros, dentre outros) e, muitas vezes, as questões referentes à segurança só se impõem a um determinado sistema quando a falta dela se torna evidente – seja por prejuízos causados, seja por sigilos quebrados ou qualquer outro problema não previsto na implementação daquele sistema. Só por isto, estudos referentes a mecanismos para ampliação de segurança em sistemas computacionais, são sempre bem vindos e, sem dúvida, necessários.

A criptografia é outra área que só tende a ganhar mais relevo nestes tempos de avanços em tecnologia digital. Desde os primórdios da teoria referente ao processamento de dados em meios mecânicos (posteriormente eletrônicos e, hoje, digitais) que a criptografia tem sido a área que mais idéias originais têm dado à “disciplina” da computação. Talvez por seu caráter estratégico na política, a criptografia sempre contou com amplo financiamento público e, às vezes, seus resultados fizeram surgir melhorias para toda a população, além dos membros da classe que detinha o poder.

Assim, a única recomendação possível é a de que os estudos, na área de criptografia e na área de segurança na rede, sejam sempre incentivados e, na medida do possível, tornados públicos, para que seus resultados se disseminem mais facilmente e propiciem avanços que tornem as tecnologias digitais acessíveis a mais pessoas, contribuindo para que a “era da informação” seja uma era de crescimento para a espécie humana.

6 REFERÊNCIAS BIBLIOGRÁFICAS

ABRANTES,A. Souza de.Patentes de Programas de Computador: **Um Estudo Dos Fundamentos de Exame E Análise De Estatísticas Do Setor,**2002. Disponível em:<http://www.nepi.adv.br/doutrina/patentes_programas.htm>Acesso em: 20 março. 2003

ALBERTIN, Alberto Luiz.**Comércio Eletrônico: Modelo, Aspectos e Contribuições de sua Aplicação**. São Paulo: Atlas, 1999.

ARNOLD, Ken, GOSLING, James.**Programando em Java.** São Paulo: Makron Books, 1997.

BARKER,Elaine; BASSHAM, Lawrence; BURR,William; DWORKIN, Morris ; FOTI, James; NECHVATAL, James; ROBACK Edward;Report on the Development of the Advanced Encryption Standard (AES).**Computer Security Division Information Technology Laboratory National Institute of Standards and Technology**, outubro.2000.Disponível em:<http://csrc.nist.gov/CryptoToolkit/aes/round2/r2report.pdf>. Acesso em: 20 março. 2003.

BERNSTEIN, Terry, BRIMANI, Ansh B. SHULTZ, Eugene, SIEGEL, Carol A.**Segurança na Internet.** Rio de Janeiro: Campus, 1997.

BITTENCOURT, Ângela.**Assinatura Digital não é Assinatura Formal.** 2002 Disponível em: <//www.modulo.com.br >, Acesso em: 02 outubro. 2002.

BITTENCOURT, Ângela.**Assinatura Eletrônica: mola mestra das comunicações virtuais.2002.** Disponível em: <http://www.modulo.com.br>Acesso em: 02 outubro. 2002.

BREVES, André.**Prazer, Java.**2002. Disponível em:<www.guj.com.br>.Acesso em:16 maio 2003.

BURNETT, Steve; PAINE, Stephe.**Criptografia e Segurança: O Guia Oficial RSA**.Rio de Janeiro: Campus, 2002.

CAMPIONE, M; WALRATH, K.**The Java Tutorial**: Object-OrientedProgramming for the Internet. [S.l.]: SunSoft Press, 1996.

CARVALHO, Moema Sá.**Fundamentação da matemática elementar**, Rio de Janeiro:Campus, 1984.

CERTISIGN.**Assinatura digital garante transações pela Internet.**Diário de São Paulo,04/02/2003. Disponível em:<http://www.certisign.com.br/imprensa>.Acesso em: 20 março. 2003.

CERTISIGN.**O Negócio é Certificação Digital,** CSO Brasil - Edição 01, 10/04/2003, Disponível em:<http://www.certisign.com.br/imprensa/2003/02042003.html>Acesso em: 20 março. 2003.

COUTINHO, S,C.**Números inteiros e criptografia RSA**. Rio de Janeiro: IMPA/SBM, 2000.

DINIZ, Davi Monteiro. Monteiro. **Documentos eletrônicos, assinaturas digitais: *da qualificação jurídica dos arquivos digitais como documentos.*** São Paulo: LTr, 1999.

DRUCKER, P.**O futuro já chegou**. Revista Exame, p.112. 2000, 22 de março.
FORD, Warwick; BAUM, Michael S.**Secure electronic commerce,** Prentince Hall,1997.

FREITAS, Daniel. M.**Segurança do Java- *Uma introdução às APIs de criptografia e assinaturas digitais.***2002. Disponível em: <http://www.modulo.com.br>Acesso em: 02 outubro 2002.

GARFINKEL, Simson.**PGP: Pretty Good Privacy. O'Reilly & Associates.** São Paulo: Market Press,1995.

GARFINKEL, Simson; SPAFFORD, Gene.**Comércio e & Segurança na Web. São Paulo**, Market Press:1999.

GOMES, Olavo José Anchiesch.**A Criminalidade Cibernética e suas Conseqüências** Legais. Reportagem de capa, Security Magazine, Ano II, Número 8, Janeiro/2001.

GONÇALVES, Marcus.**Firewalls – Guia Completo**. Rio de Janeiro: Editora Ciência Moderna Ltda.,2000.
GRANT, Gail L.**Understanding Digital Signatures***.* New York: McGraw Hill, 1998.

HAICAL, Cristiane. **Biometria: o corpo humano no processo de autenticação.**2001.Disponível em:<www.modulo.com.br>.Acesso em:20 julho 2003.

INDRUSIAK,Leandro**.LinguagemJava.**1996.Disponívelem:<http://www.inf.ufrgs.br/tools/java>.Acesso em:20 janeiro 2002.

JÚNIOR BRAGA, S. Mário.**Proposta de modelo RBC para a recuperação inteligente de jurisprudência na Justiça Federal,** 2001. Dissertação (Mestrado em Engenharia de Produção) – Programa de Pós-Graduação em Engenharia de Produção, UFSC, Florianópolis.

KAMINSKI, Omar.ICP-OAB - OAB-SP inicia a emissão dos certificados digitais. **Revista Consultor Jurídico, São Paulo, nov. 2002.** Disponível em: < http://conjur.uol.com.br/view.cfm>. Acesso em: 16 dez. 2002.

KHANNA, Raman.**Distributed Computing Implementation and Management Strategies**. Prentice Hall, 1993.

KNUDSEN, Jonathan.**Java Cryptoghaphy.**Ed. O`reilly, 1998.

KULIKOVSKY, Sérgio. **Vida nova na era digital.** 2003.Disponível em: <http://www.certisign.com.br/imprensa/2003/05062003.html>.Acesso em:15 maio 2003.

KUROSE, James F.; ROSS, Keith W.**Redes de Computadores: uma nova abordagem.** 1. ed. – São Paulo:Addison Wesley, 2003.

LINDEBERG, Sousa B.**Redes de Computadores** - Dados, Voz e Imagem, São Paulo:Erica, 1999.

LINHARES, Flávia;MOREIRA, Dilvan. A.**Interface de Segurança para Servidores de Dados Universais,** 2001.Disponível em:< http://java.icmc.sc.usp.br>.Acesso em:20 maio 2002.

LUCCA, Newton De; SIMÃO FILHO, Simão.**Direito & Internet – aspectos jurídicos relevantes.** Bauru, SP:Edipro, 2000.

LYNCH, Daniel C., LUNDQUIST, Leslie.**Dinheiro Digital: o comércio na Internet.**Tradução por: Follow-up Traduções e Assessoria de Informática. Rio de Janeiro, Campus, 1996.

NEGROPONTE, Nicholas.**A Vida Digital**. São Paulo, SP: Companhia das Letras, 1995.

NORTHCUTT, Stephen ; ZELTSER, Lenny; WINTERS, Scott ; FREDERICK, Karen Kent ; RITCHEY, Ronald W.**Desvendando Segurança em Redes - *O Guia Definitivo para Fortificação de Perímetros de Rede Usando Firewalls, Vpns, Roteadores e Sist***., Rio de Janeiro:Campus, 2002.

OAKS, Scott.**Segurança de dados em Java.** Rio de Janeiro: Ciência Moderna, 1999.

OLIVEIRA, L. Evandro.**Tecnologia de Informação e Gestão Pública: Senhas - Identificação e Autenticação para Redução de Vulnerabilidades na Rede Municipal de Informática - RMI.** Dissertação (Mestrado em Administração Pública) - Programa de Pós-Graduação em Administração Pública da Escola de Governo da Fundação João Pinheiro, UFMG, Belo Horizonte.

PANETTA, Nestor.**Criptografia,** Reportagem de capa, Security Magazine, Ano I, Número 6, Setembro/2000.

RABELO, Air.**As Organizações Virtuais e o Teletrabalho na era das grandes redes de computadores**, 2001.Dissertação (Mestrado em Engenharia de Produção) – Programa de Pós-Graduação em Engenharia de Produção, UFSC, Florianópolis.

SAWICKI, Ed.**Segurança**. Tradução por: José Paulo, Rio de Janeiro: Editora Campus, 1993.

SCHNEIER, Bruce.**Segurança . com – Segredos e mentiras sobre a proteção na vida digital**. Rio de Janeiro: Campus, 2001.

SCHNEIER, Bruce.**Applied Cryptography: protocols, algorithms, and source code in C –** 2°. ed – New Jersey,1996.

SHOKRANIAN, M. Soares; Godinho, H. **Teoria dos Números:** Brasília: Universidade de Brasília, 1999.

SILVA, Edna Lúcia; MENEZES, Estera Muszkat. **Metodologia da Pesquisa** -2° ed. - 2001. Dissertação (Mestrado em Engenharia de Produção) – Programa de Pós-Graduação em Engenharia de Produção, UFSC, Florianópolis.

SILVEIRA, Jorge.L.**Comunicação de Dados e Sistemas de Teleprocessamento.** Rio de Janeiro: Makron Books, 1991.

SILVEIRA, Paulo.**Utilizando a classe java.util.Random e aprendendo como esses números são gerados, e o que é a semente.**2002. Disponível em:<www.guj.com.br>.Acesso em:16 janeiro 2003.

STALLINGS, William.**Cryptography and Network Security:** principles and practice – 2. ed – New Jersey: Prentice Hall,1999**.**

STEIL, Rafael.**Sopa de letrinhas sabor Java.**2002. Disponível em:<www.guj.com.br>.Acesso em:16 janeiro 2003.

STOHLER,Paulo. **Criptografia: Conceitos Básicos** Segunda Parte Future Technologies**,** fevereiro. 2002.Disponível em:<http://www.fti.com.br/n_jornal/artigo_paulo_cripto02.htm>. Acesso em: 20 março. 2003.

SUN, Microsystem.**JavaTM Cryptography Extension (JCE) -** ***Reference Guide for the JavaTM 2 SDK, Standard Edition, v 1.4*****,** 2002.
Disponível
em:http://java.sun.com/j2se/1.4.1/docs/guide/security/jce/JCERefGuide.html
Acesso em: 02 abril. 2003.

SUN, Microsystem.**JavaTM Cryptography Architecture -** ***API Specification & Reference,***2002.Disponível
em:http://java.sun.com/j2se/1.4.1/docs/guide/security/CryptoSpec.html.Acesso em: 02 abril.2003.

TERADA, Routo.**Segurança de Dados: Criptografia em Redes de Computador**. São Paulo: Edgard Blucher, 2000.

VELOSO, Caio J. M.**Criptologia – Uma ciência fundamental para tratamento de informações sigilosas.**2002. Disponível em:<www.modulo.com.br>.Acesso em:20 janeiro 2003.

VOLPI, Marlon M.**Assinatura Digital** – Aspectos Técnicos, Práticos e Legais. Rio de Janeiro: Axcel Books do Brasil, 2001.

WADLOW, Thomas A.**Segurança de Redes:** Projeto e Gerenciamento de Redes Seguras. Rio de Janeiro: Editora Campus, 2000.

XEXÉO, Geraldo.**Autenticação de Documentos Digitais por Sistemas Criptográficos de Chave Pública**.2001.Disponível em:< . www.modulo.com.br >. Acesso em: 05 novembro, 2001.

ANEXOS

Anexo 1 – Exemplos de fontes de programas criados em Java para promover assinaturas digitais.

1.1 – Gerar chaves de assinatura:

```
import java.io.*;
import java.security.*;
import com.sun.crypto.provider.SunJCE;

public class Chaves {

public static void main(String args[]) {

      if (args.length != 2) {
            System.out.println("Sintaxe: java Chaves <nome de arquivo> <seed>");
            System.exit(0);
      }
      String arquivo = args[0];   // nome de arquivo onde serão colocadas as chaves
      String seed = args[1];      // "semente" ou frase-senha para geração da chave
      try {
            // criar instancia do provider SunJCE. pode ser substituído por qualquer outro provider que implemente DSA
          SunJCE jce = new SunJCE();
            // adiciona SunJCE à lista de providers
          Security.addProvider(jce);
            // instancia objeto KeyPairGenerator para gerar par de chaves do DSA
            KeyPairGenerator keyGen = KeyPairGenerator.getInstance("DSA");
```

```
            // instancia objeto de geração de números pseudo-
aleatorios para utilização em SHA1 e DSA
            SecureRandom                    random                    =
SecureRandom.getInstance("SHA1PRNG", "SUN");
            // alimenta o gerador de números pseudo-aleatorios com
a semente digitada pelo usuário
            random.setSeed(seed.getBytes());
            // inicializa o gerador de chaves com o numero pseudo-
aleatorio
            keyGen.initialize(1024, random);
            // gera par de chaves (publica e privada) a partir dos
parâmetros anteriores
            KeyPair parChaves = keyGen.generateKeyPair();
            // obtém do KeyPair as chaves publica e privada e
armazena em objetos adequados
            PublicKey pubKey = parChaves.getPublic();
            PrivateKey priKey = parChaves.getPrivate();
            // grava arquivos de chave serializando os objetos
            // o objeto serializado pode ser utilizado para
armazenamento em diversos modos, como por exemplo
            //  bancos de dados (campos BLOB), arquivos e outros
          ObjectOutputStream fpub = new ObjectOutputStream(new
FileOutputStream(arquivo+".pubkey"));
          ObjectOutputStream fpri = new ObjectOutputStream(new
FileOutputStream(arquivo+".prikey"));
          fpub.writeObject(pubKey);
          fpri.writeObject(priKey);
          fpub.close();
          fpri.close();

          System.out.println("Chaves geradas em arquivos:
"+arquivo+".pubkey e "+arquivo+".prikey");

      } catch (Exception e1) {
            System.out.println("Exceção: "+e1);
      }
  }
```

1.2 – Assinar um arquivo:

```
import java.io.*;
import java.security.*;
import java.security.spec.*;

public class Assinar {

public static void main(String args[]) {

    if (args.length != 2) {
            System.out.println("Sintaxe: java Assinar <arquivo> <arq chave privada>");
            System.exit(0);
    }

    String arquivo = args[0];    // nome do arquivo a ser assinado
            String arqPrivada = args[1]; // nome do arquivo com a chave privada

    try {
            // abrir arquivo da chave privada para leitura
            ObjectInputStream keyIn = new ObjectInputStream(new FileInputStream(arqPrivada));
            // ler objeto do arquivo (ObjectStream) e armazenar em objeto da classe PrivateKey
            PrivateKey chavePrivada = (PrivateKey) keyIn.readObject();
            // fechar arquivo
            keyIn.close();
            // abertura do arquivo a ser assinado
            FileInputStream fin = new FileInputStream(arquivo);
            // declaração de buffer para assinatura e tamanho
            byte[] buffer = new byte[8192];
            int tamanho;
            // instancia objeto de assinatura digital (Signature) baseado em DSA com SHA1
            Signature dsa = Signature.getInstance("SHA1withDSA");
```

```
            // inicializa o engine de assinatura com a chave privada fornecida
            dsa.initSign(chavePrivada);
            // ler todo o arquivo
            while ((tamanho = fin.read(buffer)) != -1) {
                  // armazena dados do arquivo no engine de assinatura
                  dsa.update(buffer, 0, tamanho);
            }
            // gera a assinatura digital, baseada nos dados inseridos a partir do arquivo
            byte[] sig = dsa.sign();

            fin.close();
            // gravação do arquivo de assinatura
            FileOutputStream signFile = new FileOutputStream(arquivo+".assinatura");
            signFile.write(sig);
            signFile.close();

            System.out.println("Assinatura em arquivo: "+arquivo+".assinatura");

      } catch (Exception e1) {
            System.out.println("Erro: "+e1);
            e1.printStackTrace();
      }

}

}
```

1.3 – Verificar a assinatura:

```
import java.io.*;
import java.security.*;
import java.security.spec.*;

public class Verificar {

public static void main(String args[]) {
    if (args.length != 2) {
            System.out.println("Sintaxe: java Verificar <arquivo> <arq chave publica>");
            System.exit(0);
    }

    String arquivo = args[0];    // nome do arquivo a ser verificado
    String arqPublica = args[1]; // nome do arquivo com a chave publica

    try {

            // leitura do arquivo de assinatura
            FileInputStream signFile = new FileInputStream(arquivo+".assinatura");
            ByteArrayOutputStream recepcao = new ByteArrayOutputStream();
            int dado = 0;
            while ((dado = signFile.read()) != -1) {
                    recepcao.write(dado);
            }
            // armazenamento da assinatura em array de bytes (sig)
            byte[] sig = recepcao.toByteArray();
            // leitura do arquivo de chave publica
            ObjectInputStream keyIn = new ObjectInputStream(new
FileInputStream(arqPublica));
            // armazena chave publica em objeto adequado (PublicKey)
            PublicKey chavePublica = (PublicKey) keyIn.readObject();
            keyIn.close();
```

```
                // abertura do arquivo a ser verificado
                FileInputStream fin = new FileInputStream(arquivo);
                // declaração de buffer para verificação e tamanho
                byte[] buffer = new byte[8192];
                int tamanho;
                // instanciação do engine de verificação
                Signature dsa = Signature.getInstance("SHA1withDSA");
                // inicialização do engine de verificação com a chave publica
                dsa.initVerify(chavePublica);
                // ler arquivo a ser verificado
                while ((tamanho = fin.read(buffer)) != -1) {
                // armazenar dados no engine de verificação
                        dsa.update(buffer, 0, tamanho);
                }
                // executar verificação de assinatura a partir dos dados do arquivo e da
assinatura (sig)
                boolean valido = dsa.verify(sig);
                if (valido) {
                        System.out.print("Assinatura valida.");
                } else {
                        System.out.print("Assinatura INVALIDA.");
                }
                fin.close();
        } catch (Exception e1) {
                System.out.println("Erro: "+e1);
                e1.printStackTrace();
        }
```