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

Valmir Vicente Minella

SISTEMA DE DISPONIBILIZAÇÃO DE DOCUMENTOS LEGAIS DE FORMA ELETRÔNICA

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

Vitório Bruno Mazzola, Dr

Florianópolis, dezembro de 2002

SISTEMA DE DISPONIBILIZAÇÃO DE DOCUMENTOS LEGAIS DE FORMA ELETRÔNICA

Valmir Vicente Minella

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

_____
Prof. Fernando A. O. Gauthier, Dr
Coordenador

Banca Examinadora

_____
Prof. Vitório Bruno Mazzola, Dr
Orientador

_____
Prof. Mário Antônio Ribeiro Dantas, Dr
Membro

_____
Prof. Roberto Willrich, Dr
Membro

À minha esposa Tânia, filhos Daniel e Ana

pelos momentos preciosos que roubei de nossa convivência

ao longo do desenvolvimento deste trabalho.

Agradecimentos

À empresa Sul Fabril por proporcionar o apoio necessário ao desenvolvimento desse trabalho e ao curso de mestrado como um todo.

Ao meu orientador, Vitório Bruno Mazzola Dr., pelo seu empenho a fim de enriquecer o trabalho e sua pronta disposição para o atendimento deste orientando.

Aos colegas de trabalho e colegas de curso pelo incentivo com vistas a atingir o objetivo proposto.

A todos os demais, não nomeados, que de forma direta ou indireta contribuíram para a realização deste trabalho.

SUMÁRIO

Lista de Figuras

Lista de Siglas

AC	Autoridade Certificadora
AH	Authentication Header
AR	Autoridade de Registro
BDB	Biblioteca Digital Brasileira
CED	Consulta e Encaminhamento para Disponibilização
CRL	Certificate Revogation List
DIGIT	Serviço de Digitalização de Documentos
DSS	Digital Signature Standard
ECN	Protocolo criptográfico para Emissão de Certidões de Nascimento na Internet
ESP	Encapsulation Security Payload
FTP	File Transfer Protocol
HTTP	Hiper Text Transfer Protocol
ICP	Infraestrutura de Chaves Públicas
ICU	Interface de Cadastro de Usuário
IP	Internet Protocol
IPSec	IP Security
ITU-T	International Telecommunication Union
LAN	Local Area Network
MAC	Message Code Authentication
MAN	Metropolitan Area Network
OAB	Ordem dos Advogados do Brasil
ODD	Órgão Disponibilizador de Documentos
PGP	Pretty Good Privacy
PKC	Public Key Certificate
PKI	Public Key Interchange
RDDE	Rede de Disponibilização de Documentos Eletrônicos
RSA	Rivest-Shamer-Adleman (desenvolvedores do algorítmo de assinatura)
SAM	Serviço Associados Manual
SDD	Serviço de Disponibilização de Documentos
SDDL	Sistema de Disponibilização de Documentos Legais

SDIC	Serviço de Disseminação de Informações Cadastrais
SEAV	Serviço Eliminador de Autenticações Vencidas
SEI	Serviço de Exportação de Informações
SII	Serviço de Importação de Informações
S/MIME	Secure Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SODD	Serviço de Obtenção direta de documentos
SRIC	Serviço Receptor de Informações Cadastrais
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TELNET	Protocolo de estabelecimento de conexão interativa
UDP	User Datagram Protocol
VAD	Verificador de Autenticidade de Documentos
VPN	Virtual Private Network
WAN	Wide Area Network
WWW	World Wide Web

RESUMO

Esta dissertação apresenta um sistema de disponibilização de documentos legais de forma eletrônica, visando proporcionar ao público em geral a obtenção facilitada de seus documentos existentes em órgãos disponibilizadores tais como cartórios ou instituições similares, sem dependência de horário de atendimento e deslocamento ao órgão detentor do documento desejado.

O sistema apresentado propõe a conversão dos documentos existentes em mídia impressa para o formato eletrônico e o armazenamento dos mesmos em bases computacionais locais do órgão disponibilizador, juntamente com documentos gerados originalmente em formato eletrônico.

As informações de documentos por usuário do órgão disponibilizador serão enviadas à um serviço centralizador de acessos, o qual fornecerá ao usuário a informação de existência de todos seus documentos em toda rede de órgãos disponibilizadores conveniados, bem como o encaminhamento do usuário ao órgão disponibilizador detentor do documento na necessidade de sua disponibilização

O uso do recurso de identidade digital, se faz necessário para controle da obtenção e autenticação dos documentos, visando adequar o sistema a normas regidas por leis que dão validade e autenticidade a documentos eletrônicos.

ABSTRACT

This dissertation shows a disponibilization system of lawful documents of electronic form, aiming provide to the public in general the facilitated obtainment of its documents that are in register office or similar institutions, without service schedule dependence and displacement to the holder organ of the document required.

The system in question propose the conversion of the existing documents in printed media for the electronic format and the storage this in databases of the register office, jointly with documents originally generated in electronic format.

The information of documents by user from the register office will be sent to a centralizer service of accesses, which will supply to the user a view of all his documents in all net of the partner register office, as well as the user guiding from the register office holder of the document when the disponibilization it's necessary.

The use of the digital resort identity, it's necessary to control the obtainment and authentication of the documents, aiming adapt the system at norms governed by laws that they give validity and authenticity of electronics documents.

1 INTRODUÇÃO

A Internet teve nos últimos anos, seu uso aumentado nos setores públicos e privados de forma notável, atingindo pessoas de várias regiões e camadas sociais sem restrição. A própria disseminação do uso de computadores, em vários segmentos antes não explorados, se deve ao interesse surgido por esta nova tecnologia, que traz o conhecimento e acontecimentos antes distantes e difíceis de serem obtidos, agora sendo acessados e conhecidos com um simples clicar de mouse, como se barreiras de tempo e espaço tivessem sido rompidas, permitindo o acesso à informação e a publicação de idéias num ambiente de alcance universal.

A explosão do uso da Internet se deve ao uso de ferramentas tais como o correio eletrônico, uma de suas primeiras ferramentas, que possibilitou a comunicação quase que instantânea entre pessoas e o uso de navegadores(browsers), que trouxe aos olhos do usuário uma informação visual de boa qualidade e com grande facilidade de acesso, inclusive encaminhando o usuário entre diversos computadores da rede, ingressando-o no que passou-se a chamar de WWW(World Wide Web), ou a teia de aranha eletrônica disseminadora de informações.

A Internet tem sido freqüente instrumento para viabilizar a desburocratização em vários segmentos públicos e privados, contando com apoio de mecanismos de armazenamento descentralizado de dados e de segurança da informação, fornecidos por diversas plataformas de computadores. A adoção destes mecanismos e ferramentas tem oferecido maior facilidade para a implementação desses recursos, pois não obriga o usuário a seguir um padrão rígido de hardware ou software.

Por exemplo, o uso da Internet no ramo bancário revolucionou o atendimento e retirou milhares de pessoas das filas de bancos. Com o uso de técnicas avançadas de segurança, trouxe ao meio da Internet um aval tecnológico de confiança ao usuário, que motivou muitos outros segmentos a acreditarem no uso eficaz da Internet para prover serviços seguros, antes somente disponibilizados utilizando-se formas tradicionais.

Mas da mesma forma que caminha a tecnologia em busca da segurança, buscando anular todas as possibilidades de corrupção da informação, caminha também em paralelo segmentos menos nobres, que tentam desenvolver técnicas para burlar os mecanismos de segurança, por mais sofisticados que sejam, através do uso de tecnologia

ou até mesmo com o uso de engenharia social, com o qual se obtém formas de acesso com o apoio de pessoas da organização.

Com o apoio das tecnologias proporcionadas pela Internet e com a existência de mecanismos avançados de segurança, vários serviços estão disponibilizados ou em projeto de disponibilização, com o objetivo de reduzir distâncias e custos na obtenção e fornecimento de informações e serviços.

O uso de tais tecnologias no apoio direto ao usuário final traz uma gratificação imediata ao desenvolvedor, no que se refere a otimizar de forma radical a obtenção de recursos antes obtidos de forma demorada e dispendiosa.

A automação de cartórios, os cartórios virtuais, tende a facilitar a vida do usuário, dos cartorários e também dos órgãos públicos, que teriam a informação centralizada, tendo um controle maior sobre a vida burocrática do país, obedecendo os limites da privacidade do usuário.

O Brasil já vem se mobilizando a algum tempo na regulamentação de transações via Internet, tais como comércio eletrônico e cartório virtual. No primeiro semestre de 2001, foi publicada a medida provisória que regulamenta a criação da ICP-Brasil (Infra-estrutura de Chaves Públicas), que dará suporte aos princípios de segurança a serem adotados por projetos futuros, em desenvolvimento em várias entidades, a serem implementados segundo sua aprovação.

1.1 Identificação do Problema

Atualmente a disponibilização de documentos físicos tais como escrituras, processos, registros, etc; tem dependência da sua obtenção em cartórios e outros órgãos, ficando o proprietário com sua posse com a finalidade futura de alguma comprovação, também fica o órgão responsável pela emissão com condições de gerar novamente o documento.

Na eventual necessidade de comprovação da existência de tal documento, geralmente o portador deverá apresentar este documento autenticado através de uma marca impressa e assinatura do órgão disponibilizador comprovando sua existência e origem.

Tal procedimento gera um trabalho de localização do documento, deslocamento ao órgão expedidor para gerar autenticação de existência do mesmo.

Levando em conta que para várias transações são necessárias várias comprovações de documentação e que nem sempre tais documentos estão na mesma cidade ou estado, temos um problema considerável de deslocamento e tempo para viabilizar um transação a ser realizada.

1.2 Estrutura da Dissertação

Este trabalho de dissertação será apresentado em 5 (cinco) capítulos.

O capitulo 2 (dois) contém uma revisão bibliográfica abordando diversos assuntos relativos à segurança da informação, acesso à sistemas computacionais, publicação de informações, validade de documentos e autenticação eletrônica e legislação aplicável.

O capítulo 3 (três) apresentará o sistema de disponibilização de documentos legais de forma eletrônica proposto, definindo alguns conceitos e descrevendo o sistema de forma sintetizada e detalhada.

No quarto capítulo será especificada a arquitetura do sistema, funcionalidades, considerações sobre tecnologias empregadas, detalhado o funcionamento dos serviços componentes software do sistema, efetuado comparação com outros sistemas, abordado a aplicação do sistema proposto em uma situação real e exposto formas de ataque e falhas do sistema levantadas e medidas de contenção previstas.

A dissertação é finalizada com o capítulo 5 (cinco), que são as considerações finais, onde serão abordadas as vantagens e desvantagens do sistema proposto em relação ao método tradicional, também são relatadas limitações de desenvolvimento, seguido de indicadores dos possíveis trabalhos futuros a serem desenvolvidos.

1.3 Perguntas de Pesquisa

As perguntas consideradas relevantes no contexto desta dissertação são abordadas abaixo. No ínterim de desenvolvimento deste trabalho foram concebidas respostas a estas perguntas.

Pergunta: Qual o contigente de usuários interessados na utilização deste recurso?
Resposta: O número de usuários que venham a utilizar este recurso, dependerá exclusivamente da quantidade e qualidade das informações disponibilizadas ao usuário, bem como a facilidade de acesso, e principalmente o fator custo do uso desta infra-estrutura, comparado com o custo de obtenção por métodos tradicionais.

Quanto maior for a integração com fornecedores de informação tais como: prefeituras, cartórios em geral, órgãos públicos, maior será o contigente de informações disponibilizadas e integradas e maiores seriam as vantagens de uso e interesse do usuário de se adequar à esta nova tecnologia.

Pergunta: Investimento utilizado versus benefício obtido?
Resposta: O retorno de investimento depende diretamente das informações disponibilizadas e da facilidade de acesso à este recurso. A popularização do uso de tecnologias é o que faz viabilizar o retorno do investimento e modernizações.

Pergunta: Forma de disponibilizar acesso facilitado a este recurso ao público geral?
Resposta: A disseminação do uso de computadores em órgãos públicos e instituições tais como escolas, propiciam formas de acesso facilitadas ao público em geral.

A implantação de terminais públicos de acesso à Internet é uma forma eficiente de popularizar o uso de futuras aplicações desenvolvidas por órgãos públicos, com a intenção de desburocratizar procedimentos, e minimizar o problema de atendimento ao público em geral .

Pergunta: Quais as garantias de segurança de informações e privacidade do usuário?
Resposta: A garantia de privacidade sobre as informações do usuário dependem de constantes evoluções de tecnologia de segurança, armazenamento e disponibilização, visando coibir a ação maliciosa de Hackers.

Outro fator a ser levado em conta, seria a seriedade dos órgãos públicos e privados envolvidos na disponibilização de tais informações, mas este problema não surge com o uso desta nova tecnologia, mas já existe da mesma forma com o uso dos métodos tradicionais de disponibilização de informações.

Pergunta: Que tipo de controle o governo teria sobre a vida do cidadão? Seria interessante este tipo de controle?

Resposta: Com o surgimento de novas tecnologias e com a popularização de seu uso, novas formas de controle do governo sobre a população são possíveis. O atual uso do sistema bancário, cartões de crédito, cartões magnéticos, e até celulares, fornecem recursos vastos de investigação da vida financeira e até do deslocamento do cidadão dentro do país.

A infra-estrutura de cartório virtual, com certeza fornece facilidades de levantamento de informações sobre o cidadão anteriormente dependente de deslocamento físico do órgão público interessado

Mas, mesmo utilizando os modos convencionais o governo pode ter acesso a tais informações, mesmo que despenda maior tempo em sua obtenção.

1.4 Objetivo Geral

O objetivo deste trabalho é apresentar um sistema de disponibilização de documentos legais de forma eletrônica, que venha desburocratizar o acesso do público em geral à documentação de sua propriedade, de forma rápida, segura e confiável, sem dependência de horário de atendimento e deslocamento físico, utilizando a Internet como meio de acesso ao sistema, contando com apoio de tecnologias recentes de segurança e apoiando-se em leis que regem a validade de assinatura digital e de documentos eletrônicos.

1.5 Objetivos Específicos

- Rever questões jurídicas relativas à validade e autenticidade de documentos eletrônicos.
- Levantar tecnologias de segurança que melhor atendam os requisitos necessários.
- Levantar tecnologias de armazenamento e disponibilização a serem empregadas.
- Conceber um sistema utilizando as tecnologias levantadas que viabilize o acesso e disponibilização de documentos de forma eletrônica ao usuário.

- Descrever funcionamento de serviços componentes do sistema que tenham necessidade de serem desenvolvidos, para suprir automação de operações específicas do projeto.
- Utilização de um órgão centralizador de requisições do usuário, a fim de facilitar a obtenção de informações sobre documentos e regulamentar a atividade dos órgãos disponibilizadores conveniados.
- Uso da Internet como meio de comunicação do sistema, como forma de popularizar o uso do sistema..
- Manter compatibilidade aproximada de uso do sistema com métodos tradicionais.

1.6 Resultados esperados

Contribuir para popularização do uso de identidade digital e validade de documentos eletrônicos.

Desburocratizar o acesso dos usuários à seus documentos, podendo o mesmo comprovar a autenticidade sem submeter-se a deslocamentos desnecessários e restrições de atendimento.

A proposição de um sistema computacional ao ser analisado por terceiros pode levar à proposições de melhorias a este trabalho que venham a servir de referência para projetos novos ou existentes.

Dar aval público à confiabilidade das tecnologias de segurança.

Quanto mais tecnologias eletrônicas que visem a desburocratização forem concebidas e adotadas, mais atrativos serão oferecidos ao usuário exigindo identidade digital do mesmo. Com o crescimento do uso novos órgãos disponibilizadores entrarão no meio oferecendo mais recursos.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Ataques / Ameaças

A utilização de computadores para armazenar e processar informações gera a necessidade do uso de mecanismos de proteção para salvaguardar a integridade e confidencialidade dos dados. As preocupações com segurança se intensificam quando nos deparamos com a utilização de tecnologias de sistemas distribuídos, onde através de redes locais(LANs), geograficamente distribuídas(WANs) e metropolitanas(MANs), compartilham-se dados entre computadores utilizando-se inclusive arquiteturas de rede tal como a Internet (TCP/IP), que deixam a desejar no que diz respeito à segurança de acesso e integridade dos dados.

Desta forma podemos definir duas formas de segurança:

- Segurança de computador, preocupada com aspectos locais no que diz respeito à invasão do sistema computacional por meio de vírus eletrônicos, acesso indevido ao sistema e a serviços não autorizados, captura, destruição e modificação de informação armazenada, entre outras.
- Segurança de rede, que tem como alvo proteger os dados que trafegam entre computadores, proporcionando serviços de confidencialidade, autenticação integridade, não repudio, disponibilidade.

Para se definir as necessidades de segurança de uma organização e avaliar os vários produtos existentes, o responsável pela segurança necessita considerar três aspectos de segurança da informação conforme [STA 99]:

- **Ataques à segurança**: qualquer ação que comprometa a segurança da informação
- **Serviço de Segurança:** Serviço que aumenta a segurança do processamento de dados e informação transferida de uma organização.
- **Mecanismos de segurança:** mecanismo desenvolvido para detectar, prever ou recuperar-se de um ataque de segurança.

2.1.1 Ataques à segurança

Nenhum sistema de informações está livre de ataques, seja o sistema de uso local ou interligado através de uma rede.

A invasão que se caracteriza pelo sucesso de um ataque é realmente a prova de que houveram falhas na concepção do sistema de segurança. Estas falhas comprometem a integridade de um sistema de informações e embaraça publicamente os profissionais de segurança, a organização provedora do serviço e até a reputação de algum produto comercial de segurança que esteve envolvido no processo.

Ataques na segurança de um sistema de computador ou rede podem ser categorizados em relação ao seu efeito, baseando-se em [STA 99]:

- **Interrupção**: tem como resultado a interrupção da informação e pode ser causado pelo corte de uma linha de comunicação, quebra de componentes de hardware ou desativação do servidor provedor de tal serviço ou de serviços de informação.
- **Interceptação:** ocorre quando uma pessoa ou programa não autorizado ganha acesso a uma informação. Difícil de ser reconhecida este tipo de fraude.
- **Modificação:** Ocorre quando a informação é interceptada, modificada e retransmitida. Fácil coibir mas seus efeitos podem ser desastrosos.
- **Fabricação:** Informações são fabricadas e inseridas no sistema, causando falha de autenticidade nas informações do sistema.

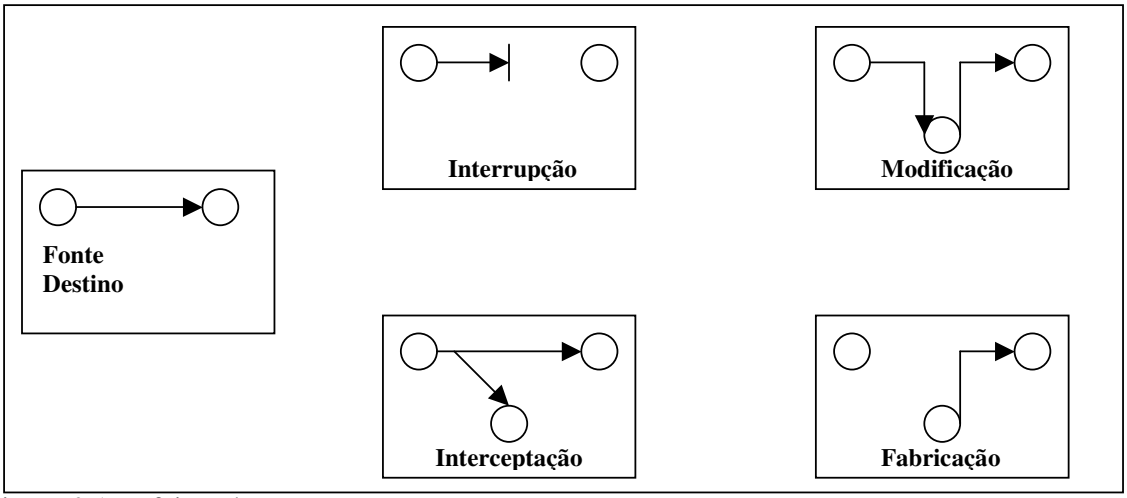

Figura 2.1: Efeitos de ataque.

Os ataques também podem ser categorizados quanto a sua forma em ataques passivos e ataques ativos.[STA 99].

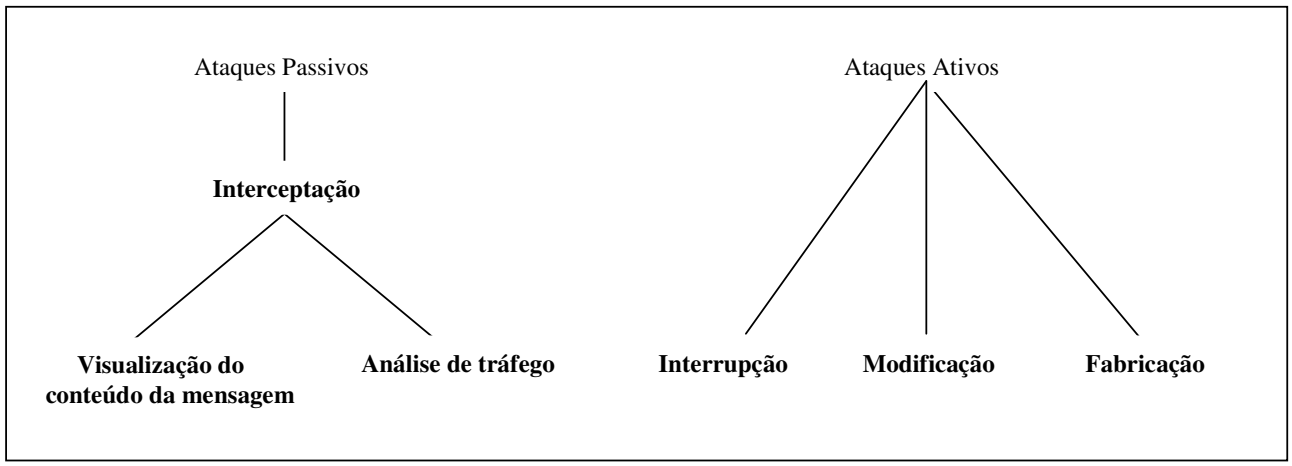

Figura 2.2: Ataques passivos e ativos

Ataques passivos: A interceptação de uma mensagem com a finalidade de conhecimento do seu conteúdo, ou análise de tráfego em busca do reconhecimento de padrões de criptografia a fim de decodificar mensagens criptografadas que trafegam pela rede, podem ser classificados como ataques passivos.

A característica de não alteração da mensagem interceptada torna o ataque passivo muito difícil de ser detectado, mas caso seja detectado sua coibição geralmente é simples de ser implementada.

Ataques ativos: Ao contrário dos ataques passivos, tem efeitos destrutivos sobre os dados, modificando ou criando dados falsos. Os ataques ativos podem ser subdivididos em quatro categorias[STA 99]:

- **Mascaramento:** ocorre quando uma entidade se faz passar por outra a fim de receber mensagens ou privilégios não destinadas à ela. A viabilização desta técnica pode ser feita pela captura de seqüências de autenticação pela entidade falsa, a qual responde ao requisitante com uma seqüência de autenticação válida forjada.
- **Repetição:** através da captura passiva e retransmissão de dados produzindo um efeito não autorizado.

- **Modificação:** ocorre com a alteração da mensagem provocando falhas no entendimento da mensagem ou servindo de meio para negar ou prover acesso indevido.
- **Negação de serviço:** pode ser negado acesso à uma pessoa ou à um serviço como um todo, através de mecanismos que provoquem sobrecarga ou desativação total ou parcial da rede ou serviço.

A gravidade de um ataque passivo ou ativo em uma entidade depende das conseqüências que um ou outro provocam. Ataques passivos não destruem informações, porém o roubo de informações pode prejudicar uma entidade tanto ou mais do que os efeitos que causam um ataque ativo, o qual é mais fácil de ser detectado.

2.1.2 Serviços de Segurança

Os serviços de segurança tem com objetivo detectar, prevenir e recuperar um sistema na ocorrência de um ataque de segurança[STA 99]. As funções requeridas para prover segurança à um sistema de informação podem ser agrupadas dentro seis classificações de serviços de segurança.

- **Confidencialidade:** serviço que deve prover proteção contra ataques passivos, ou seja, qualquer informação trafegada não deve ser visualizada por pessoas não autorizadas, isso pode ser viabilizado através do uso de canais virtuais de comunicação e técnicas criptográficas .
- **Autenticação:** deve garantir que a origem da comunicação seja autêntica, que os envolvidos, terminal acessando e servidor respondendo, ambos tenham certeza da identidade do parceiro e que não haja possibilidade de haver mascaramento de origem ou destino com o objetivo de receber ou prover informações indevidas. Com a utilização criptografia e identidade digital torna-se possível garantir a identidade.
- **Integridade:** A integridade positiva de uma informação prova que ela não foi alterada, duplicada, gerada, reordenada ou respondida. Serviços de integridade orientada a conexão garantem estas exigências bem como detectam destruição de dados e negação de serviço.

- **Não repudio:** Este serviço fornece a prova de que a mensagem foi realmente enviada e recebida. Nem o emissor pode negar que enviou a mensagem, nem o receptor pode negar que a recebeu.
- **Controle de acesso:** tem por função controlar o acesso à um sistema de informação, identificando, autenticando e dando direitos de acesso individual a cada usuário.
- **Disponibilidade:** devem coibir ataques que reduzam ou cessem a disponibilidade do sistema.

2.1.3 Mecanismos de segurança

Diversas tecnologias foram desenvolvidas visando atender às várias exigências da segurança da informação e acesso. Os serviços de segurança para atenderem os requisitos exigidos utilizam-se de um ou mais mecanismos descritos ao longo deste capítulo.

2.2 Criptografia

Criada a milhares de anos por civilizações antigas, usada inclusive no âmbito militar proporcionava o envio de instruções de guerra às forças de batalha provendo segurança da informação, pois mesmo sendo interceptada pelo inimigo não podia ser lida de forma natural

Estes sistemas antigos eram baseados em duas técnicas: substituição e transposição [GAR 99]. A substituição baseia-se no princípio de substituir cada letra da mensagem por outra. A transposição baseia-se na mistura dos caracteres da mensagem.

A criptografia de uma mensagem consiste em transformar uma mensagem legível, em uma seqüência de caracteres sem sentido lógico, com o uso de uma técnica reversível, onde somente o destinatário da mensagem com o conhecimento do mecanismo de criptografia utilizado poderia decodificar a mensagem, obtendo assim acesso ao seu conteúdo original.

O uso da criptografia abstraindo o conteúdo da mensagem, além de evitar o conhecimento de seu conteúdo por possíveis invasores, também evita que tal informação sofra alteração de seu conteúdo sem conhecimento do receptor, pois o

invasor necessitaria conhecer o processo de criptografia para decodificar a mensagem, alterá-la e codificá-la novamente.

Além dos mecanismos de criptografia para codificar uma mensagem, utiliza-se uma seqüência de bits chamada chave de criptografia, que tem como função fornecer uma personalização do processo, dificultando de forma expressiva o conhecimento das técnicas utilizadas e possibilitando que o destinatário da mensagem possa reverter o processo de cifragem. A decifragem é o processo inverso pelo qual o texto cifrado é transformado no texto limpo usando-se uma segunda função complexa e uma chave de decifragem [GAR 99]. A chave de decifragem em alguns sistemas criptográficos é igual a chave de criptografia, mas em outros são diferentes.

Tal processo de cifragem e decifragem de um texto é representado abaixo.

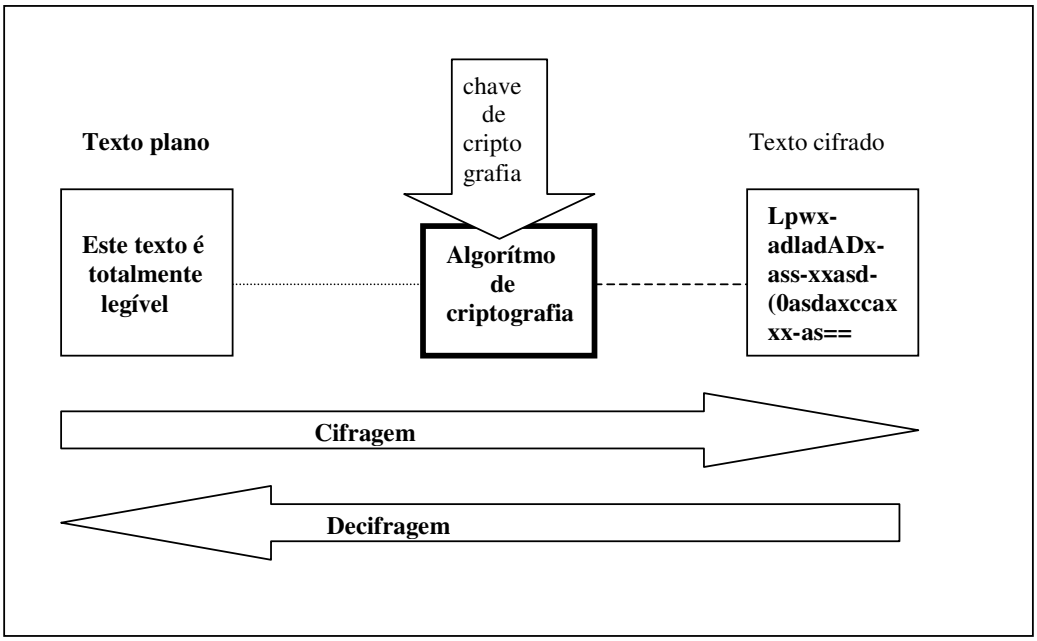

Figura 2.3: Exemplo de cifragem e decifragem de um texto utilizando-se algorítmo de criptografia com chave.

Sendo o texto plano **X**, a chave de criptografia **K** e o texto cifrado **Y** podemos representar:

o processo de encriptação **E** como: $Y = E_K(X)$

o processo de decriptação **D** como: $X = D_K(Y)$

2.2.1 Criptografia Simétrica

O algorítmo de chave simétrica usa um método que a chave de criptografia é utilizada para encriptar e também decriptar o texto plano, em alguns casos a chave de decriptação não é a mesma, mas é obtida com base na chave de encriptação.

São utilizados geralmente para criptografar dados e fluxos de dados, pois são rápidos e possuem um nível de segurança quase perfeita em algumas implementações.

Os algoritmos de chave simétrica podem ser divididos em duas categorias: de bloco e de fluxo. Algoritmos de bloco criptografam os dados um bloco de cada vez, enquanto os algoritmos de fluxo criptografam byte por byte.[GAR 99]

Várias técnicas de viabilização da criptografia simétrica geram grande confiabilidade deste método, inclusive melhorias contínuas nestas técnicas, fazem que técnicas de criptoanálise se tornem inviáveis num período de tempo. Diferentes algoritmos oferecem diferentes níveis de segurança, este nível depende da dificuldade de quebra do mesmo[SCH 96].

Segundo [GAR 99] há muitos algoritmos de chave simétrica em uso atualmente. Alguns dos algoritmos mais comuns no campo de segurança web são sucintamente descritos abaixo:

DES: Padrão de Criptografia de Dados (Data Encryption Standard), é um algorítmo de bloco que usa uma chave de 56 bits. Sua segurança de quebra está fragilizada nos últimos tempos vítima da evolução do poder computacional.

Triple-DES: Utilizando-se o algoritmo de criptografia DES convencional três vezes com três chaves diferentes obtém-se pelo menos duas vezes mais segurança em relação ao uso singelo do DES.

Blowfish: Algoritmo de criptografia em bloco, rápido compacto e simples, inventado por Bruce Schneier. Permite uso de chave de tamanho variável até 448 bits.

IDEA: Usado pelo programa PGP para criptografar arquivos e correio eletrônico usa uma chave de 128 bits e é bastante poderoso.

RC5: Desenvolvido por Ronald Rivest, permite que o tamanho da chave, o tamanho dos blocos e o número de vezes que a criptografia será realizada sejam definidos pelo usuário.[GAR 99]

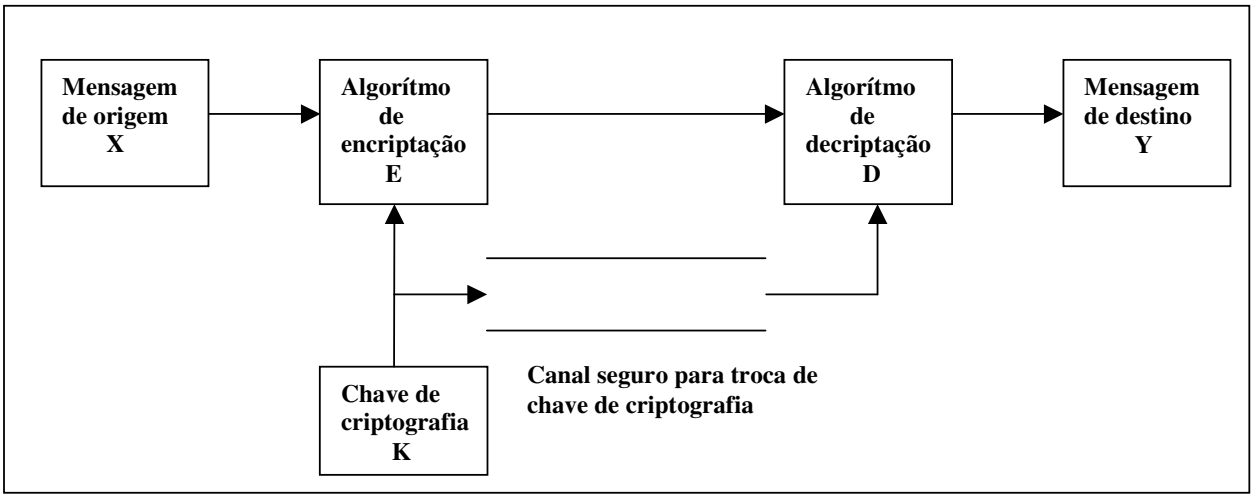

Figura 2.4: Criptografia simétrica com troca segura de chaves [STA 99]

2.2.2 Criptografia Assimétrica

Outro tipo de criptografia baseada em chave seria a criptografia assimétrica, ou criptografia de chave pública, que utiliza chaves diferentes para encriptar e decriptar o texto, sem que estas chaves tenham relação entre elas. As chaves são obtidas por meio de funções matemáticas ao invés de substituições e permutações tal como na criptografia simétrica, sendo computacionalmente impraticável determinar a chave de decriptação tendo somente o conhecimento do algoritmo de criptografia e a chave de encriptação [STA 99].

No processo de criptografia de chave pública um sistema gera um par de chaves usados para encriptar e decriptar mensagens. A chave pública de encriptação é divulgada publicamente pelo órgão gerador e a chave privada é fornecida somente ao usuário de forma secreta. Uma pessoa que queira enviar um texto confidencialmente de forma criptografada a um usuário destino, com posse da chave pública deste usuário destino, criptografa a mensagem com a chave pública e utilizando o algoritmo assimétrico relativo. Esta mensagem só poderá ser decodificada com o uso da chave privada do usuário destino, que somente ele tem conhecimento.

A criptografia assimétrica também possibilita o recurso de assinatura de uma mensagem, ou seja, o receptor pode ter certeza que a mensagem foi enviada por uma determinada pessoa. Este recurso é viabilizado pelo emissor, com posse de sua chave

privada, encriptando a mensagem. Qualquer pessoa de posse da chave pública deste emissor poderá decriptar a mensagem, tendo certeza da sua origem, pois a chave privada é de conhecimento somente do emissor.

A Figura 2.5 demonstra o processo que provê confidencialidade na troca de mensagens, onde a origem A envia a mensagem X para o destino B, encriptando a mesma com a chave pública KUb do destino B de conhecimento público.
O destino B recebendo a mensagem Y criptografada utiliza sua chave privada KRb de seu uso particular para decriptar a mensagem.

processo de encriptação $Y = E_{KUb}(X)$
processo de decriptação $X = D_{KRb}(Y)$

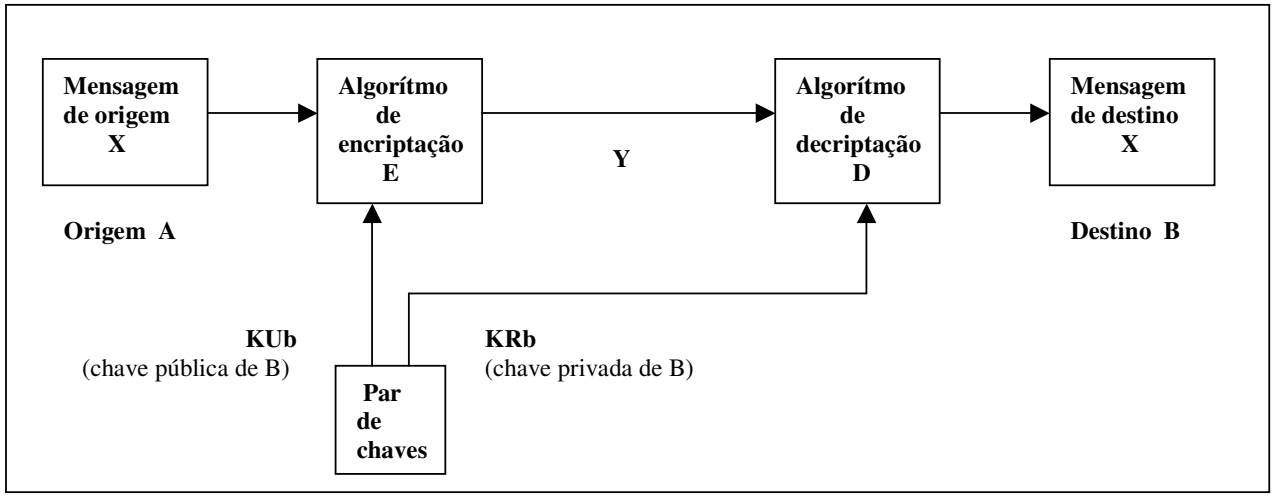

Figura 2.5. Criptografia assimétrica (confidencialidade)

A Figura 2.6 demonstra o processo que provê autenticidade na emissão de uma mensagem, onde a origem A envia a mensagem X para o destino B, encriptando a mesma com a sua chave privada KRa de seu conhecimento particular.
O destino B recebendo a mensagem Y criptografada utiliza sua chave pública KUa da origem A de conhecimento irrestrito para decriptar a mensagem. Sendo que somente a origem A tem conhecimento de sua chave privada, o destino B terá certeza da identidade do emissor, origem A.

Representação matemática:

- processo de encriptação $Y = E_{KRa}(X)$
- processo de decriptação $X = D_{KUa}(Y)$

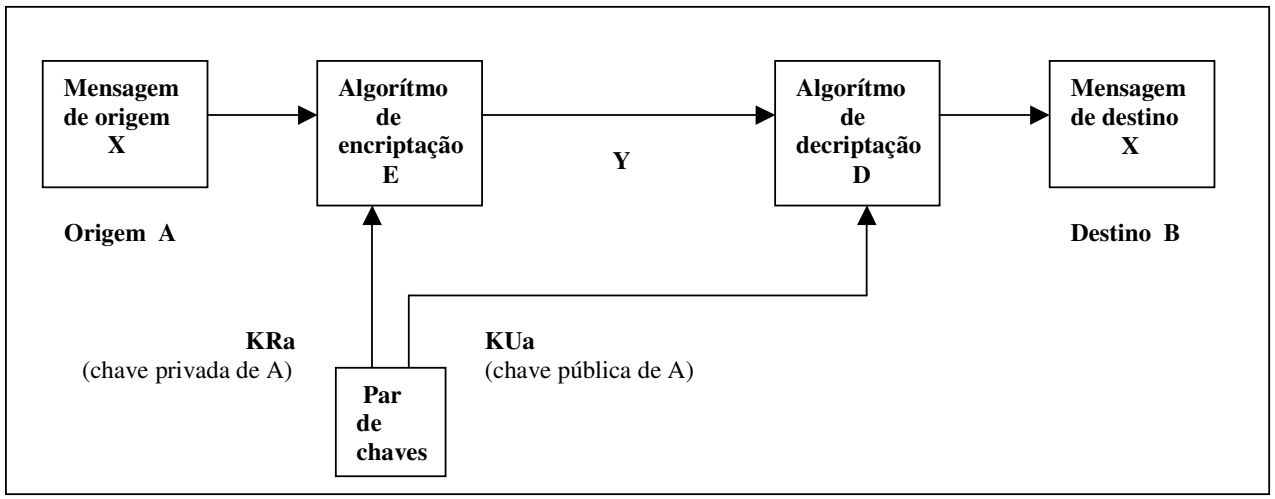

Figura 2.6. Criptografia assimétrica (autenticidade) [STA 99]

Podemos agregar as facilidades de autenticidade e confidencialidade providas pela criptografia assimétrica a fim de obter uma mensagem segura com origem comprovada utilizando os seguintes procedimentos.

O emissor A:

- encripta (E) a mensagem com a sua chave privada (KRa) a fim de gerar autenticidade.
- encripta (E) a mensagem gerada pelo passo anterior com a chave pública (KUb) do receptor B obtendo a mensagem encriptada Y, a fim de gerar confidencialidade.

O receptor B:

- decripta (D) a mensagem Y com a sua chave privada (KRb) obtendo a mensagem X de origem com confidencialidade garantida.
- decripta (D) a mensagem obtida pelo passo anterior com a chave pública do emissor A (KUa), obtendo a mensagem X e comprovando a autenticidade da mesma.

Representação matemática:

encriptação: Y=EKUb[EKRa(X)]

decriptação: X=DKUa[DKRb(Y)]

2.2.3 Criptoanálise

O termo criptoanálise é oriundo da palavra *kriptós* que tem o significado de oculto, em junção com a palavra *análysis* com significado de decomposição e define a arte ou ciência de descobrir o texto original legível ou a chave de criptografia tendo somente posse do texto cifrado e/ou conhecimento do algorítmo de criptografia utilizado.

O sucesso de uma criptoanálise pode recuperar o texto plano ou a chave. Ele também pode achar fragilidades no criptosistema que eventualmente conduzem à resultados anteriores [SCH 96]. Uma tentativa de criptoanálise pode ser definida como um ataque à um criptosistema.

Os ataques comuns relativos à um algoritmo de criptografia com objetivo de quebrar sua segurança obtendo a decifragem dos dados sem o conhecimento da chave de criptografia ou seja técnicas de criptoanálise, são descritas abaixo:

- **Ataque de força bruta:** consiste no uso de poder computacional com o objetivo de testar todas as chaves criptográficas possíveis até que se consiga decifrar a informação criptografada, para isto deve-se conhecer o algorítmo de criptografia utilizado. A única defesa contra este ataque é tentar dificultar a descoberta da chave de criptografia, utilizando-se maior tamanho de chave possível, o que pode comprometer a performance do criptosistema.
- **Análise de criptografia:** Os ataques à um sistema criptográfico o qual buscam a chave utilizada no processo de criptografia são raros. Geralmente utiliza-se a criptoanálise diferencial que consiste em escolher textos planos, criptografá-los e comparar semelhanças dos efeitos nestes textos com outros textos criptografados, buscando levantar algoritmos de criptografia e/ou chaves utilizadas.

Um ataque à um sistema de criptografia pode ter dois objetivos possíveis: a descoberta do texto original a partir de um texto criptografado ou a descoberta do algoritmo de criptografia utilizado a partir de um texto criptografado. Segundo [GAR 99] os ataques abaixo são usados geralmente quando o algoritmo criptográfico é conhecido:

- **Ataque do texto conhecido**: neste caso o analista dispõe de um bloco de texto original e o mesmo bloco criptografado. Conhecendo o algoritmo de criptografia ele pode usar estas relações para obter facilmente a chave de criptografia utilizada.
- **Ataque ao texto escolhido:** o analista criptografa um texto geralmente utilizado no meio de comunicação em questão e compara com a mensagem criptografada que trafega neste meio. Quando houver comparação positiva com a mensagem original codificada e a mensagem gerada pelo analista, descobre-se a chave utilizada para decodificar o restante da comunicação.
- **Análise de criptografia diferencial:** Tipo de ataque ao texto escolhido que se faz criptografando textos um pouco diferentes um do outro e comparando resultados.
- **Análise diferencial de falha:** Consiste em se provocar uma falha em um dispositivo de criptografia de hardware, sendo que a partir dos efeitos causados por esta falha na decodificação de uma informação venham a ser levantados padrões de criptografia utilizados.
- **Ataques baseados no sistema:** Atacando o sistema criptográfico que usa o algoritmo de criptografia pode gerar condições de quebra do código sem ter como alvo o algoritmo de criptografia utilizado.

Como acontece com a criptografia convencional, a criptografia de chave pública também é vulnerável ao ataque de força bruta [STA 99]. O uso de chaves de criptografia de tamanho grande torna computacionalmente inviável este tipo de ataque, mas torna o processo de criptografia muito lento.

Outra forma de ataque à criptografia de chave pública é a tentativa de obter a chave secreta com base na chave pública através do fatoramento de um número associado à chave pública. O sucesso deste tipo de ataque não está matematicamente descartado, sendo suspeitos até mesmo os mais avançados algoritmos como o RSA.

Todos estes ataques descritos se enquadram dentro do conceito de criptoanálise e tendem a comprometer a confidencialidade da informação em qualquer criptosistema, mas segundo [SCH 96] se o custo requerido para quebrar o texto cifrado for maior do que o valor do dado encriptado ou se o tempo requerido para quebrar o texto cifrado for mais longo do que o tempo que o dado deve permanecer secreto, não há necessidade de preocupação excessiva relativo à ataques envolvendo criptoanálise.

As técnicas de criptografia e criptoanálise juntas compõe uma ciência chamada de criptologia (*criptós*=oculto + logo=ciência), sendo os estudiosos possuídores de conhecimento matemático avançado.

Mesmo sendo campos opostos tanto a criptografia como a criptoanálise obtém avanços expressivos relativos ao desenvolvimento de novas de técnicas de ataque e proteção à sistemas criptográficos

2.2.4 Algoritmo RSA

O RSA desenvolvido em 1977 por Ron Rivest, Adi Shamir e Len Adleman ou seja, o Rivest-Shamer-Adleman (RSA) , é atualmente o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. O RSA utiliza números primos.

A algoritmo RSA se baseia na facilidade de multiplicação de dois números primos para obter um terceiro número e na dificuldade de recuperar os dois primos a partir daquele terceiro número.

Gerar a chave pública envolve multiplicar dois primos grandes. Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Assim, a segurança do RSA baseia-se na dificuldade de fatoração de números grandes, o qual requer recursos computacionais avançados e tempo elevado.

2.3 Confidencialidade e Autenticidade de uma mensagem

A troca de informações entre dois pontos para ser considerada segura deve atender os requisitos de confidencialidade e autenticidade, ou seja, somente os envolvidos no processo de transmissão podem ter conhecimento do conteúdo da mensagem e certeza da origem e autenticidade da mesma.

Autenticação é um método que garante que uma mensagem foi realmente enviada pela origem alegada e não sofreu qualquer tipo de modificação em trânsito. Para proporcionar a segurança mencionada um sistema eficaz deve atender a requisitos de segurança que visem coibir certos tipos de ataques.

No contexto de comunicação através de uma rede, os seguintes ataques podem ser identificados. [STA 99]

- Visualização da mensagem: por pessoas ou processos não autorizados.
- Análise de tráfego: em busca de padrões de comunicação que dêem condições de sincronia dos ataques.
- Mascaramento: inserção de mensagens na rede a partir de fonte fraudulenta.
- Modificação do conteúdo: usando inserção, exclusão e modificação.
- Modificação de seqüência: além da modificação da seqüência entre partes, também a exclusão e reordenação das mensagens.
- Modificação temporal: atrasos ou repetição de mensagens.
- Repúdio: Negação de envio ou recebimento de uma mensagem.

O processo de criptografia convencional pode oferecer características básicas que proporcione confidencialidade e autenticidade à uma mensagem.

A criptografia simétrica provê confidencialidade e autenticidade na transmissão de uma mensagem. Sendo que o emissor A criptografa uma mensagem utilizando uma chave de conhecimento do receptor B, esta mensagem chega confidencialmente ao receptor B. Ao descriptografar a mensagem além de receber a mensagem confidencial também o receptor B tem a garantia que foi realmente o emissor A que enviou a mensagem pois somente A e B tem conhecimento da chave de criptografia.

No entanto a agilidade de comunicação deste processo fica comprometida pela dificuldade de compartilhamento da chave de criptografia entre emissor e receptor. O quesito repúdio não pode ser atendido pois tanto o emissor pode negar o envio quanto o receptor negar o recebimento, pois a chave de criptografia é compartilhada não tendo relação de identidade.

Na criptografia assimétrica tal com descrito no capítulo 2 item 2.2.2 a autenticidade é obtida com a criptografia da mensagem a ser enviada com a chave privada do emissor e a confidencialidade é obtida com a criptografia do produto da mensagem criptografada anteriormente com a chave pública do receptor.

Exemplificando, o receptor descriptografa primeiramente a mensagem recebida usando sua chave privada fechando o ciclo da confidencialidade e depois de posse da

chave pública do emissor descriptografa o produto anterior obtendo a comprovação de autenticidade da fonte de envio.

A desvantagem deste processo está na utilização do algoritmo de chave pública o qual é muito complexo, por quatro vezes para prover confidencialidade e autenticidade gerando um tempo de processamento excessivo, exigindo um poder computacional relativamente grande para prover agilidade ao processo.

2.3.1 Técnicas de Autenticação de mensagem

2.3.1.1 Código de Autenticação da Mensagem - MAC

Pelo fato de a criptografia de chave pública ser lenta, não é uma boa idéia encriptar o texto simples inteiro[BUR 02] e sim criar um resumo deste texto e utilizar técnicas para prover autenticidade baseadas neste resumo.

Uma alternativa de prover autenticidade envolve o uso de uma chave secreta para gerar um pequeno bloco de dados de tamanho fixo[STA 99] ou resumo, que é inserida no final da mensagem, conhecida como MAC (Message Autentication Code).

Esta técnica assume que A e B compartilham uma chave K. Quando A deseja enviar uma mensagem para B, A utilizando uma função geradora de MAC e a chave K gera o MAC da mensagem que é agregada à mensagem original e enviada ao receptor. O receptor separa a mensagem recebida do MAC e recalcula o MAC, ai então comparando o MAC recebido com o MAC calculado. Se forem iguais, tem-se certeza de que a mensagem não sofreu qualquer tipo de alteração.

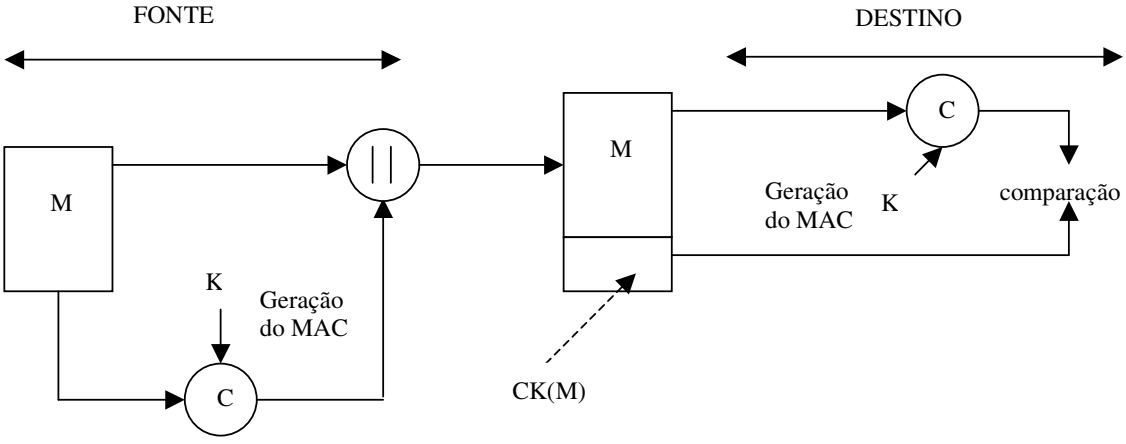

Figura 2.7: Código de Autenticação da Mensagem - MAC

Este processo provê autenticação, mas não provê confidencialidade, pois a mensagem trafega na forma de texto legível.

A Figura 2.8 demonstra uma forma de prover também confidencialidade ao processo, onde o texto legível e o MAC calculado no envio são criptografados usando uma segunda chave de conhecimento mútuo antes do envio. No recebimento é realizada a decifragem da mensagem obtendo-se o MAC e a mensagem legível, com os quais é viabilizado o processo de comparação de MAC recebido e calculado.

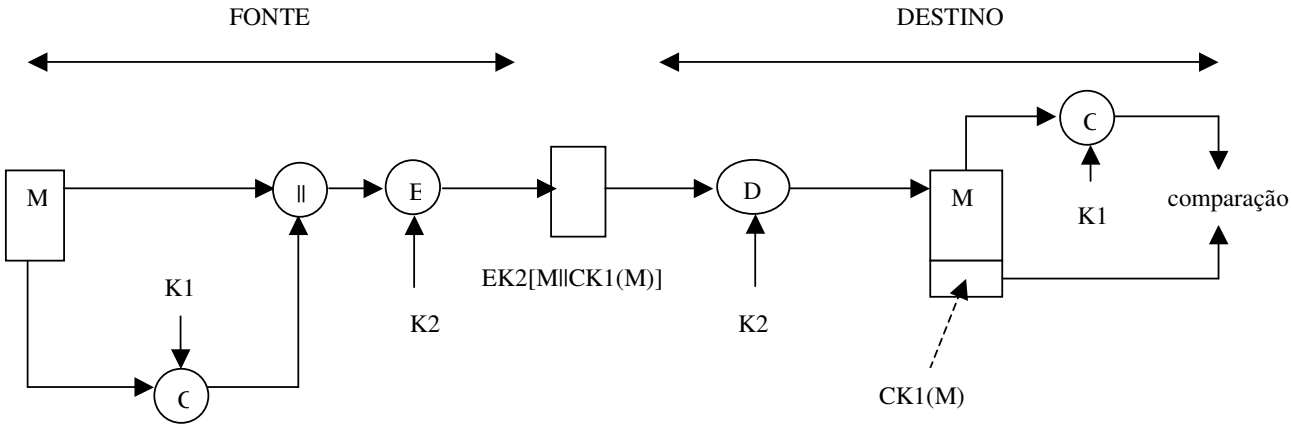

Figura 2.8: Código de Autenticação da Mensagem – MAC com confidencialidade.

O processo de Código de Autenticação de Mensagem tal como o processo de criptografia simétrica não provê o recurso de assinatura digital, pois a chave utilizada na geração do MAC e a chave utilizada na criptografia e descriptografia são compartilhadas entre o emissor e o receptor da mensagem.

2.3.1.2 Função HASH

Uma variação do Código e Autenticação de Mensagem (MAC) são as funções HASH que tal como o MAC fornecem a partir de uma mensagem de tamanho variável, um código HASH de tamanho fixo. A geração do código HASH envolve todos os bits da mensagem, ou seja, a modificação de qualquer bit da mensagem resulta em mudança no código HASH. Como a geração do código HASH não envolve uso de chaves secretas, se faz necessário agregar segurança na transmissão do código HASH, pois caso

contrário, qualquer um que tenha poder do mecanismo de geração do código HASH poderia inserir uma mensagem com seu respectivo HASH no meio de transmissão.

A Figura 2.9 abaixo demonstra um mecanismo utilizando HASH, criptografia de chave pública e criptografia simétrica provendo tanto autenticidade, assinatura digital e confidencialidade.

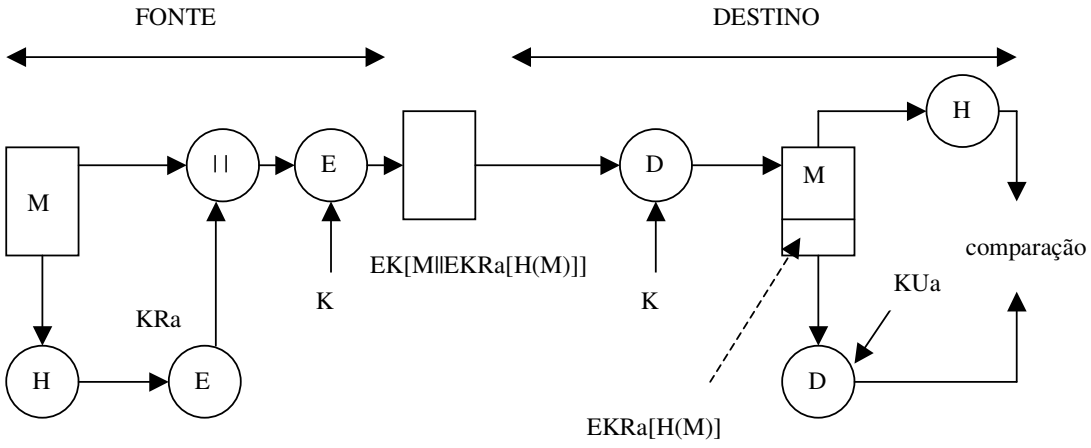

Figura 2.9: Hash com confidencialidade, autenticidade e assinatura digital.

Emissor	.gera código hash (H) da mensagem.	H(M)
	.criptografa o código hash gerado.	EKRa[H(M)]
	.agrega código hash gerado com mensagem legível em criptografa ambos com chave (K) compartilhada entre emissor e receptor.	EK[M||EKRa[H(M)]]
Receptor	.Descriptografa mensagem criptografada recebida	DK[M||EKRa[H(M)]]
	Obtendo mensagem legível (M) e	EKRa[H(M)]
	.Descriptografa DKUa[H(M)] obtendo	H(M) recebido
	.A partir da mensagem legível (M) gera o código HASH e compara o código HASH recebido com o código HASH calculado.	H(M) calculado

Se ocorrer sucesso em todo o processo, inclusive sendo o código HASH recebido igual ao código HASH calculado, temos garantido confidencialidade, autenticidade e assinatura digital.

2.3.2 Considerações

A autenticação de uma mensagem protege duas partes que trocam mensagens, de uma terceira parte. Todavia, não protege as duas partes entre elas [STA 99].
Podemos usar como exemplo os casos abaixo levantados:

- Um dos envolvidos num processo de transmissão pode forjar o recebimento de uma mensagem, ou seja, ele próprio cria a mensagem, gera o código de autenticação com o uso da chave compartilhada com seu parceiro de transmissão e pode alegar numa disputa que esta mensagem foi gerada por seu parceiro.
- Em outro caso pode ser negado o envio de uma mensagem. O autor do envio da mensagem pode alegar que a mensagem não foi enviada por ele e sim forjada pelo receptor tal como analisado no caso acima.

2.4 Assinatura Digital

Em casos que não existe relação de confiança entre os envolvidos os processos que proporcionam autenticidade não são suficientes.

A tecnologia de assinatura digital é a solução mais recomendada para solucionar estes problemas. A assinatura digital é análoga à assinatura manual e deve ter as seguintes propriedades [STA 99]:

- Deve ser possível verificar o autor, data, e hora da assinatura.
- Deve ser possível autenticar o conteúdo na hora da assinatura.
- A assinatura deve ser prover condições de ser analisada por uma terceira parte com a finalidade de resolver disputas.

Além das propriedades citadas acima que visam compatibilizar a assinatura manual com a assinatura digital, devem ser atendidas outras condições para que o processo de assinatura digital seja viável:

- O processo de produção, reconhecimento e verificação de uma assinatura digital deve ser simples.
- Não deve ser computacionalmente possível forjar uma assinatura.
- A assinatura efetuada deve ser baseada no conteúdo da mensagem.
- O armazenamento de uma assinatura digital deve ser possível.
- Não pode haver duas assinaturas idênticas.

A Figura 2.9 que utiliza função HASH segura, criptografia assimétrica e criptografia simétrica atendem estes requisitos.

2.4.1 Categorias

Uma variedade de formas tem sido propostas para a função de assinatura digital. Estas formas dividem-se em duas categorias[STA 99]:

2.4.1.1 Assinatura digital direta

Assume que tanto a chave pública do emissor quanto a do receptor sejam divulgadas publicamente. O emissor criptografa a mensagem ou o seu código HASH gerado com sua chave privada provendo autenticidade. Caso somente o código HASH tenha sido criptografado e a mensagem esteja legível e se queira prover confidencialidade, o emissor deve criptografar o código HASH assinado mais a mensagem legível com a chave pública do receptor.

Em caso de disputa uma terceira parte deve ter o conhecimento da mensagem assinada para comprovação. Se a mensagem além de criptografada com a chave privada do emissor para prover autenticidade, for criptografada com a chave pública do receptor para prover confidencialidade, então necessita da intervenção do receptor na transformação da mensagem cifrada recebida em mensagem legível agregada ao código HASH assinado pelo emissor, agora sim com possibilidade de ser verificada a assinatura do emissor.

Um dos problemas da assinatura digital direta é o caso de uma das partes negar o envio de uma mensagem alegando que houve perda de sigilo da sua chave privada. Este

problema pode ser contornado incluindo-se uma marca de tempo junto com a assinatura e utilizando-se assinaturas com tempo de vida limitado.

2.4.1.2 Assinatura digital arbitrada

Os problemas associados com a assinatura digital direta podem ser resolvidos com a inserção de um mecanismo arbitro que tenha relação de confiança com o emissor e receptor. Este mecanismo têm como função testar o conteúdo e originalidade da mensagem.

O emissor da mensagem em vez de enviá-la assinada diretamente para o receptor, envia para um árbitro. Este por sua vez checa o conteúdo e originalidade da assinatura repassando a mensagem para o receptor agregando uma indicação de conformidade e data.

2.4.2 Padrão de Assinatura Digital - DSS

O DSS utiliza um algoritmo de hash e um algoritmo de assinatura digital avançado e é desenhado para prover somente a função de assinatura digital[STA 99], não pode ser usado para encriptação ou exportação de chaves, tal como o padrão RSA.

Descrevendo o funcionamento do RSA conforme Figura 2.10, a fim de efetuar comparações temos os seguintes passos efetuados:

.envio da mensagem

- A mensagem a ser assinada é submetida à uma função hash que produz um hash seguro de tamanho fixo (H).
- Este código hash seguro é então encriptado com a chave privada do emissor (KRa), formando a assinatura.
- Esta assinatura gerada e a mensagem original são enviadas ao receptor.

.recebimento da mensagem

- O receptor gera um código hash (H) a partir da mensagem recebida
- Decripta a assinatura recebida utilizando a chave pública do emissor (KUa) obtendo código hash gerado pelo emissor.

- Compara o código hash gerado por ele com o código hash gera pelo emissor. Se forem iguais a assinatura é valida, e a mensagem recebida é confiável também em relação ao seu conteúdo.

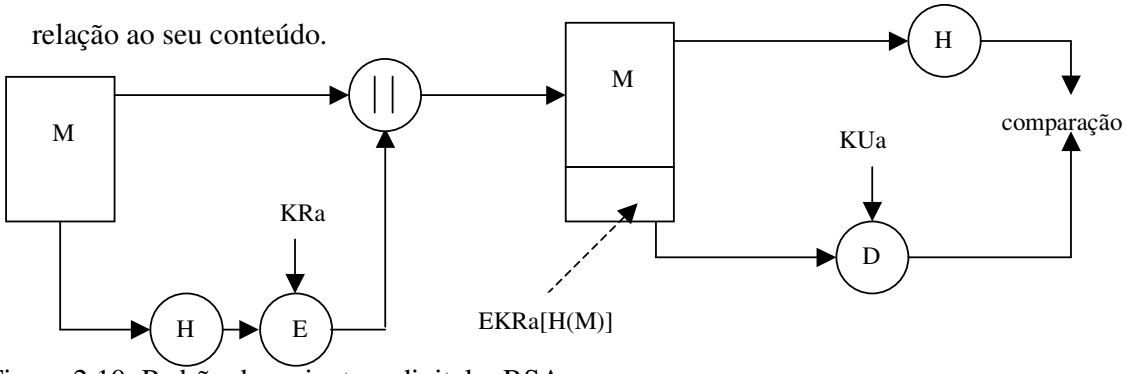

Figura 2.10: Padrão de assinatura digital – RSA

Descrevendo o funcionamento do DSS conforme Figura 2.11.

. *envio da mensagem*

- é gerado o código hash (H) da mensagem a ser assinada
- o código hash gerado serve como entrada para a função de assinatura (Sig) juntamente com um número randômico **k** gerado, a chave privada do emissor KRa e uma chave KUg, chave pública global gerando como produto dois componentes chamados **s** e **r**.
- os componentes **s** e **r** mais a mensagem original são enviados para o receptor.

. *recebimento da mensagem*

- no recebimento é gerado o código hash (H) da mensagem recebida.
- este código hash gerado mais os componentes **s** e **r** recebidos, a chave pública do emissor KUa e a chave global pública KUg servem de entrada para a função de verificação de assinatura (Ver), que irá gerar um componente **r,** o qual sendo igual ao componente **r** recebido comprova a validade da assinatura.

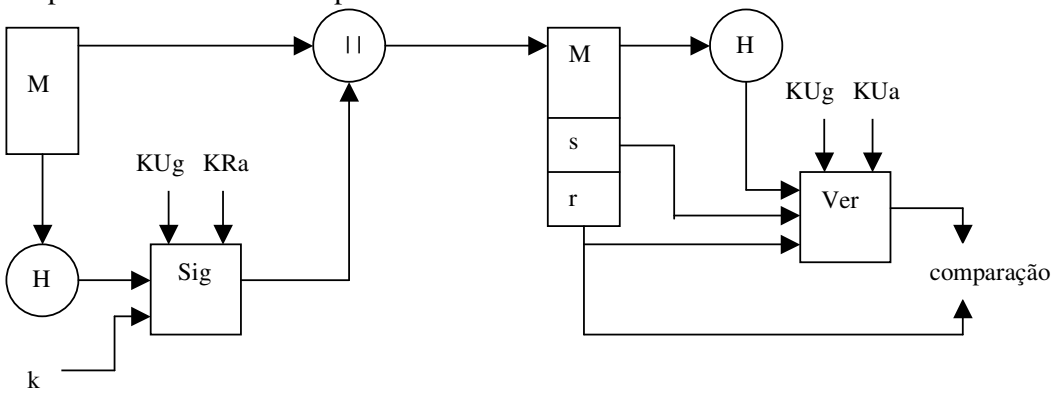

Figura 2.11: Padrão de assinatura digital - DSS

O mecanismo de assinatura digital utilizado no DSS comparativamente com o RSA provê um acréscimo significativo de segurança pois envolve mais componentes integrados na geração e verificação da assinatura.

2.5 Infraestrutura de chaves públicas - ICP

Conhecida mundialmente como PKI (Public Key Infrastructure) a ICP tem a finalidade de fornecer um certificado digital agregado à uma chave pública que identifica um usuário. O funcionamento da ICP baseia-se na confiança que os envolvidos em um processo de identificação tem que ter na Autoridade Certificadora (AC), aquela que emite o certificado digital.

A implementação de uma ICP envolve uma Autoridade certificadora (AC) que é responsável pela emissão do certificado digital e identificação do usuário final, por uma Autoridade de Registro (AR) que é opcional, mas se existir serve de intermediária entre a AC e o usuário final identificando usuários de forma mais abrangente, e por repositórios de certificados e CRL onde ficam armazenados os certificados emitidos e cancelados e podem ser acessados por todos usuários.

2.5.1 Autoridade Certificadora - AC

Em uma ICP, uma AC emite, gerencia e revoga certificados para uma comunidade de usuários finais [BUR 02]. Estes certificados são assinados pela chave privada da autoridade certificadora e contém informações da pessoa, sua chave pública, um número serial e outras informações e atesta que uma determinada chave pública pertence a um indivíduo ou empresa específica.

A chave pública do usuário pode ser facilmente recuperada tendo o interessado posse da chave pública da AC emissora publicamente divulgada e acessando a AC. Estes certificados são armazenados em repositórios de certificados sem necessidade cuidados especiais, pois seu conhecimento pode ser público.

Uma AC pode ser implementada em vários meios com finalidades distintas conforme [GAR 99]:

- AC interno: de uso restrito interno de uma empresa poderia certificar seus funcionários e níveis de autorização, servindo como base única para controle do acesso a seus sistemas computacionais.
- AC de um funcionário terceirizado: utiliza-se do mesmo conceito da AC interno, mas tal serviço de certificação seria oferecido por uma empresa terceirizada.
- AC de cliente terceirizado: Os clientes de uma empresa poderiam se utilizar dos certificados digitais que esta empresa fornece para estabelecer relação comercial confiável, mas em vez da empresa arcar com os custos e trabalho de implementação de tal estrutura, confia esta prática à uma empresa terceirizada confiável.
- AC de terceiros confiável: A operação da autoridade certificadora fica a cargo do governo ou empresa especializada. Isto possibilita que indivíduos sem nenhuma relação anterior possam confiar entre si baseando-se na confiança em relação à autoridade certificadora.

A emissão de certificados com valor legal têm que ser autorizada por órgãos reguladores. Qualquer entidade utilizando softwares gratuitos pode emitir certificados, mas o seu valor legal numa transação eletrônica pode ser contestado.

Um órgão certificador com autorização legal para emissão de certificados tem que ser certificado por um órgão certificador de hierarquia superior para que seja garantida a validade legal dos certificados emitidos por ele.

A AC é no final responsável pela autenticidade de seus usuários finais [BUR 02].

Um erro na emissão de um certificado pode causar problemas graves atingindo clientes e fornecedores que tenham utilizado tal certificado numa transação eletrônica, podendo haver disputas jurídicas com grande envolvimento da AC emissora do certificado digital.

O uso da certificação digital no mundo tem crescido de forma gradativa e várias empresas têm se consolidado no mercado mundial tais como Baltimore, Entrust e Verisign, sendo que a Verisign posui uma representação brasileira chamada Certisign.

2.5.2 Autoridade de Registro - AR

Como descrito anteriormente, a AR é opcional dentro de uma ICP, mas está se tornando uma necessidade pois alivia a carga de trabalho de uma AC com o crescimento de usuários utilizadores de certificados digitais.

Uma AR pode servir como um entidade intermediária entre a AC e seus usuários finais, ajudando a AC em suas funções rotineiras para processamento de certificados [BUR 02]. Uma AR geralmente exerce as funções de:

- Verificação dos documentos apresentados pelo cliente no ato da inscrição.
- Geração das chaves públicas e privadas.
- Armazenamento e recuperação do certificado em cartões tais como SmarCard.
- Pedido do cancelamento do certificado ou chave privada a pedido do cliente junto com a AC.
- Armazenamento de chaves privadas de forma segura a pedido do cliente.

2.5.3 Revogação de certificados

A lista de certificados cancelados (CRL Certificate Revogation List) tem como função armazenar os certificados que por algum motivo foram cancelados e deve ser consultada cada vez que seja envolvida em uma transação eletrônica. Em sua forma básica, uma CRL é uma estrutura dados assinada contendo uma lista de data/hora dos certificados revogados [BUR 02]. Além de listar os certificados que foram revogados, a CRL informa por quanto tempo ela será válida e como obter uma nova CRL [GAR 99].

Um certificado digital pode ser cancelado por vários motivos. Alguns motivos são relacionados:

- Chave privada do usuário é extraviada, roubada ou estava sendo confiada à uma pessoa que passou a não ser mais confiável.
- Erro na emissão do certificado pela própria AC.
- Fraudes internas na AC que comprometeram a emissão de certificados
- Mudança significativa dos dados do certificado por parte do usuário
- Qualquer motivo que venha a comprometer a legitimidade do certificado.

Segundo [GAR 99] o uso das CRLs é muito interessante na teoria, mas na prática apresentam alguns problemas:

- As CRLs tendem a crescer de tamanho constantemente gerando dificuldade na obtenção e consulta.
- Entre o tempo de revogação de um certificado, inclusão na CRL e distribuição da mesma, podem ocorrer consultas à este certificado, dando parecer que ele ainda é válido.
- Informações contidas nas CRLs podem ser utilizadas para análise de tráfego.

Uma alternativa que pode ser usada para resolver tais problemas seria disponibilização de uma consulta em tempo real à uma base centralizada de CRLs, mas esta solução também pode ser prejudicada caso o site da AC que disponibiliza esta informação esteja fora de atividade ou haja congestionamento na rede.

2.5.4 Certificados digitais ou certificados de chave pública

Um certificado de chave pública (public-key certificate – PKC) é um conjunto de dados à prova de falsificação que atesta a associação de uma chave pública à um usuário final [BUR 02], fornecendo um método confiável para distribuição de chave pública a ser executado por uma AC.

O certificado X.509 v3 é um padrão popular para certificados de chave pública [GAR 99] , definido de acordo com o padrão X.509 da ITU-T (International Telecommunication Union) com característica que permite que pares de nome/valor arbitrários possam ser incluídos no certificado padrão.

Os principais elementos de um certificado X.509 v3 são descritos abaixo:

- Versão: identifica a versão do certificado padrão X.509 (versão 1,2 ou 3)
- Número serial do certificado: valor numérico único atribuído pela AC.
- Identificador de algoritmo de assinatura: informa o algoritmo e parâmetros utilizados para assinar o certificado.
- Nome do emissor: nome da AC que criou e assinou o certificado
- Validade (Não antes/Não depois): período de validade do certificado, inicio e fim.
- Nome do sujeito: nome do usuário a quem este certificado se refere.

- Informações sobre a chave pública do sujeito: a chave pública do sujeito, junto com a identificação do algoritmo com o qual esta chave pode ser usada.
- Identificador único do emissor: elemento usado para identificar se a AC emissora é única.
- Identificador único do sujeito: elemento usado para identificar se o sujeito é único
- Extensões: conjunto de uma ou mais informações de extensão. As extensões foram implementadas na versão 3.
- Assinatura: elemento que protege todos os outros campos do Certificado. Contém o código hash dos outros campos, cifrado com a chave privada da AC, e a identificação do algoritmo de assinatura.

A Figura 2.12 conforme [BUR 02] mostra a estrutura do certificado X.509 V.1 e campos agregados das versões 2 e 3.

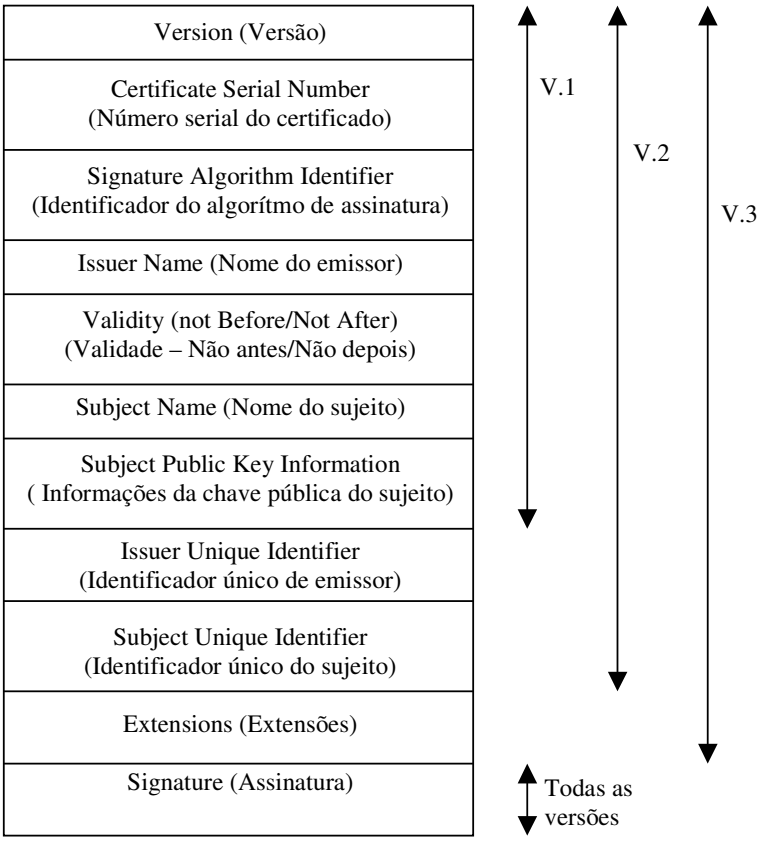

Figura 2.12: Estrutura do certificado X.509.

2.6 Legislação aplicável

Muito está sendo discutido a nível nacional sobre a regulamentação do comércio eletrônico, cartório virtual e infra-estruturas que dão suporte à estas atividades.

O governo tomou frente elaborando, e aprovando decretos e medidas provisórias a fim de regulamentar tais atividades. Estas medidas nem sempre agradam todos os segmentos envolvidos, gerando polêmicas quanto a alguns detalhes que dão poderes de controle ao governo, considerados centralizadores e autoritários por algumas entidades tal como a OAB (Ordem dos Advogados do Brasil).

Mas com certeza, mecanismos reguladores de atividades que envolvam transações via Internet, tem de ser criados para dar suporte à disputas jurídicas que envolvam comércio eletrônico, que garantam a autenticidade, integridade e a validade jurídica de documentos eletrônicos, de aplicações e realização de transações eletrônicas seguras.

2.6.1 Documentos tradicionais versus documentos eletrônicos.

Documento tradicional conforme existe à milhares de anos tem a função de representar a descrição de um fato ocorrido, que deve ser do conhecimento de mais de uma pessoa.

O aceite de seu conteúdo se faz com aplicação de uma marca, geralmente assinatura física biométrica dos participantes, fazendo parte de seu conteúdo e com possibilidade de comprovação visual de sua autenticidade, seja por pessoas normais ou de forma mais apurada por especialistas que levantam as características pessoais da assinatura, seja na sua forma e intensidade de escrita.

Tal documento habitualmente conhecido sempre se apresentou de forma física, seja em papel ou qualquer outro material que tenha possibilidade de receber marcação física duradoura, com possibilidade de reconhecimento visual imediato.

Com a evolução das tecnologias eletrônicas de processamento e armazenamento de dados surgiu a possibilidade de gerar documentos de forma eletrônica, com facilidades de armazenamento e recuperação otimizados, sem o problema do envelhecimento físico do documento tal como acontece nos meios tradicionais.

Questões jurídicas apontam fragilidades nos quesitos integridade, autenticidade e recuperação perene de um documento eletrônico.

Tecnologicamente podem ser garantidas soluções comprovadas para os problemas relacionados, mas mesmo assim existem divergências quanto ao ponto de vista da validade de um documento eletrônico, principalmente no que se diz respeito a comprovação de autenticidade da assinatura dos envolvidos na geração do documento, pois no modo tradicional fica comprovada a presença física dos envolvidos através da assinatura manual com caracterização inclusive biométrica na maneira que é impressa a assinatura no meio físico, além da verificação gráfica.

Já a assinatura eletrônica baseia-se exclusivamente na confiança que se tem na autoridade certificadora que garante a identidade do envolvido, e num possível conhecimento restrito da chave privada pelo seu proprietário, a qual é a base da identificação.

Pareceres como estes dividem a opinião dos envolvidas na regulamentação definitiva da validade dos documentos eletrônicos de forma abrangente, inclusive há duas interpretações jurídicas quanto à validade de documentos eletrônicos. Uma delas nega a possibilidade jurídica do documento eletrônico, a outra que subdivide-se em duas sendo que a primeira admite sem restrições a validade do documento eletrônico e a segunda que somente aceita se forem cumpridos alguns requisitos, dada a sua volatilidade e falta de marca biométrica que dê personalidade ao processo, tipo assinatura convencional.

O projeto de lei nº 4906 de 2001 baseado no projeto de lei nº 1483 de 1999 que trata sobre assinatura digital em transações eletrônicas e no projeto de lei nº 1589 de 1999 que trata de validade jurídica dos documentos eletrônicos e assinatura digital, tem sua atenção dada ao comércio eletrônico em geral , ao reconhecimento jurídico das mensagens eletrônicas, e abordas questões sobre validade de documentos eletrônicos.

O artigo 3º deste projeto de lei reconhece sendo original um documento eletrônico digitalmente assinado pelo seu autor e reconhece como cópia a digitalização de um documento físico existente com possibilidade de recuperação perene. Desta forma conclui-se que a digitalização de um documento físico seguido de uma assinatura digital pode servir como prova em transações comerciais, com aval de órgãos reguladores.

A validade de um documento eletrônico não poderá ser repudiada pelo fato de que o certificado digital foi emitido por uma autoridade certificadora não credenciada, de acordo com o artigo 5º , esta resolução libera o comércio eletrônico e outras transações eletrônicas a escolher autoridades certificadoras não credenciadas sem no entanto sofrer complicações jurídicas em disputas.

Em uma transação eletrônica que envolva compromisso temporal, o registro da data de efetivação da assinatura de um documento por envolvidos deve ser viabilizada através de algum parâmetro, pois como descrito no artigo 6º qualquer um dos signatários pode comprovar ao contrário por todos meios de direito.

A validade de um documento eletrônico assinado digitalmente pode ser questionada em juízo caso sejam apresentadas provas de falhas no processo de criptografia e assinatura de um documento eletrônico utilizando processos que obtenham a chave privada do signatário a partir de sua chave pública ou análise do conteúdo assinado, conforme abortado no artigo 8º . Qualquer prova de que haveria formas de assinar em nome de uma pessoa sem posse de sua chave privada teria repercussão catastrófica mundial, pois além de poder ser invalidada judicialmente as assinaturas efetuadas utilizando esta tecnologia, levaria ao descrédito qualquer forma de assinatura digital, pois os usuários tendem a tachar a eficiência de uma tecnologia baseando-se no sucesso ou fracasso de uma de suas implementações.

A comprovação de identidade em relação à Autoridade Certificadora no ato da inscrição do usuário é feita de forma tradicional, com presença física, assinatura manual, arquivamento de documentos físicos, sendo que todo este procedimento é base de comprovação de processos judiciais como relatado no artigo 11º . Atualmente não poderia ser feito de outra forma, somente com uma mudança no processo de identificação pessoal no ato do nascimento, com uma possível captura de informações biométricas aliado a um cadastro computadorizado e a informatização de todos os órgãos interessados, é que poderíamos atribuir uma identidade digital à uma pessoa desde o nascimento, não necessitando a conversão futura de identidade convencional para identidade digital.

Ao usuário do certificado digital caberá o dever de fornecer informações verdadeiras no ato do cadastro na Autoridade certificadora, caso contrário poderá sofrer penalidades judiciais; guardar com sigilo sua chave privada e comunicar imediatamente

a quebra de seu sigilo à autoridade certificadora para ser incluída na lista de revogação, conforme descrito no artigo 13º . Os cuidados com uma chave privada que identifica o usuário são realmente maiores do que temos com a assinatura convencional. Não conseguimos provar com facilidade que um documento foi assinado indevidamente através da posse furtiva por terceiros de nossa chave privada. Já falsificações de assinatura manual são facilmente detectadas por peritos, restando somente tomar precauções com incidentes que nos forcem a assinar documentos contra nossa vontade.

O artigo 19º responsabiliza civilmente a autoridade certificadora por danos causados ao titular e a terceiros devido à falsificação de certificados por ela emitidos. A falha de procedimentos operacionais na ligação de uma chave privada à um certificado e falha no processo de assinatura levando à quebra de sigilo e falsificações de assinatura são exemplos que podem levar uma autoridade certificadora a ter que ressarcir os envolvidos.

Um documento eletrônico assinado de acordo com requisitos desta lei, ao ser transmitido entre duas partes com endereços acordados, no ato do recebimento terá o mesmo peso de expedição tal como uma carta registrada com ou sem aviso de recebimento, tal como relatado nos artigos 27º e 28º . Estes artigos tendem a garantir o não repúdio no recebimento e envio de um documento.

Este projeto lei trata ainda de pontos que dizem respeito à defesa do consumidor, sigilo de informações trafegadas na rede, penalidades relativas à contravenções descritas neste projeto lei , dando suporte ao direcionamento jurídico de disputas que venham a ocorrer.

2.6.2 Regulamentação da Infra-estrutura de chaves públicas

A ICP-Brasil (Infraestrutura de Chaves Públicas) foi criada pela Medida Provisória 2200, de 28 de junho de 2001 (última reedição em 24 de agosto de 2001) com a finalidade de garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, bem como a identidade dos donos e órgãos emissores de documentos e transações eletrônicas, sendo sua aplicação destinada não somente à órgãos públicos, mas também na validação de transações eletrônicas convencionais.

Utilizando a criptografia de chave pública aliada a certificados digitais fornece meios de comprovar a autenticidade de pessoas e documentos em uma transação eletrônica tal como acontece com as infraestruturas de chaves públicas já implementadas no âmbito nacional e internacional.

A regulamentação da assinatura eletrônica e da estrutura de certificação digital tem como objetivo desburocratizar o relacionamento do governo com a sociedade, investidores, mercado e fornecedores.

A ICP-Brasil será implantada sob a coordenação de um Comitê Gestor de Políticas, vinculado à casa civil da Presidência da República. Este comitê estabelecerá políticas, critérios e normas para o licenciamento das autoridades certificadoras e de registro que comporão a ICP-Brasil e poderá negociar e aprovar acordos de cooperação internacional no que diz respeito certificação bilateral ou cruzada e regras de interoperabilidade .

A autoridade máxima de certificação, a Certificadora Raiz (AC Raiz) será exercida pelo Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e da Tecnologia. Abaixo da AC Raiz estão as Autoridades Certificadoras (AC) e Autoridades de Registro (AR) que são responsáveis por emitir e divulgar certificados digitais.

A AC Raiz será responsável por divulgar as políticas de certificados e normas técnicas e operacionais aprovadas pelo comitê gestor da ICP para as ACs e ARs e será responsável por controlar certificados das mesmas, fiscalizá-las, auditá-las e gerenciar a lista de certificados emitidos, cancelados e vencidos. A AC Raiz somente está impedida de emitir certificados para o usuário final, deixando esta tarefa para as ACs e ARs.

A medida provisória 2200 de 28 de junho de 2001 após adotada com força de lei sofreu repúdio acentuado de várias entidades, enfatizando a OAB (Ordem dos Advogados do Brasil).

As críticas da OAB e outros segmentos resultaram numa segunda edição desta medida provisória, a MP 2200-1 de 27 de julho de 2001 que veio solucionar problemas de privacidade do usuário final, maior participação da sociedade civil e limitações do poder do Comitê Gestor.

O § único do artigo 8^{o} da MP 2200-1 veio solucionar o problema de privacidade na geração do par de chaves criptográficas do usuário final que na versão

anterior da MP 2200 era de responsabilidade da AC, o que feria os princípios de privacidade pois a AC teria conhecimento da chave privada do usuário final. Com esta mudança o par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle uso e conhecimento.

Alvo de muitas críticas o governo através da reeditada MP 2200-1 no seu artigo 3º aumentou o número de representantes da sociedade civil de 4 para 5 acalmando as demonstrações de repúdio à MP 2200 e demonstrando interesse em compartilhar a tomada de decisões quanto ao estabelecimento de regras e protocolos.

Sendo que artigo 9º estabelece que a AR deve exigir a presença dos usuários no ato do cadastro restringe-se de forma considerável a possibilidade de fraudes durante o cadastro com a exigência de documentos e presença física do usuário.

A medida provisória em questão não obriga que se utilize a ICP-Brasil para que um documento particular tenha autenticidade comprovada, podendo ser utilizados outros meios de prova de autenticidade, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento com relata o § 2 º do artigo 12º da MP. Isto é um ponto positivo no que diz respeito ao desenrolar do comércio e transações eletrônicas existentes em geral, mas a padronização de uso da estrutura da ICP-Brasil nos órgãos governamentares acabam impondo sua utilização nos setores privados pois o governo tende a ser ainda um dos maiores fornecedores e cliente comercial e industrial.

No que diz respeito a veracidade das informações dispostas em um documento eletrônico o § 1º do artigo 12º da MP2200-1 limita os efeitos legais da certificação ao próprio signatário se baseando no artigo 131 da lei nº 3.071, 1º de janeiro de 1961 – Código civil.

O artigo 10º dispõe do licenciamento de órgãos e entidades públicas e pessoas jurídicas de direito privado para funcionarem como AC ou AR, desde que atendam os requisitos impostos pela Comitê Gestor. Isto capilariza a disseminação da tecnologia de identidade digital, pois o credenciamento de órgãos tais como cartórios existentes em todas cidades torna o acesso ao público em geral mais facilitado na medida em que novos produtos que exijam identidade digital forem sendo oferecidos.

A Medida Provisória MP 2200-1 veio aparar arestas da MP 2200 resolvendo questões fundamentais que asseguram privacidade, segurança e liberdade dos cidadãos

no que diz respeito ao uso do meio eletrônico e definição de regras de funcionamento da estrutura de certificação.

2.7 Sistemas criptográficos

A tecnologia Worl Wide Web tem alavancado a disseminação e criação de novas tecnologias de segurança. Vários sistemas criptográficos foram desenvolvidos e espalhados pela rede a fim de prover a segurança necessária.
Os sistemas criptográficos em uso podem ser divididos em duas categorias [GAR 99].

O primeiro grupo trata da segurança das mensagens de correio eletrônico através de programas e protocolos criptográficos , tais como:

2.7.1 Pretty Good Privacy - PGP

O PGP é sistema criptográfico híbrido, que usa criptografia de chave pública RSA para gerenciamento de chave e criptografia simétrica IDEA para cifragem dos dados brutos [GAR 99].

2.7.2 Secure Multipurpose Internet Mail Extensions – S/MIME

De propriedade da RSA Data Security este protocolo além da função de envio de arquivos binários na Internet realizado pelo MIME (Multipurpose Internet Mail extensions) o S/MIME, Secure MIME aceita correio eletrônico criptografado.

O segundo grupo tem como função oferecer confidencialidade, autenticação, integridade e não-repúdio exigindo comunicação em tempo real entre cliente e servidor. Descreve-se dois sistemas criptográficos deste grupo abaixo:

2.7.3 Secure Socket Layer – SSL

É um protocolo de uso geral para o envio de informações criptografadas pela Internet [GAR 99], fornecendo um canal seguro com confidencialidade, autenticação,

integridade e não-repúdio da informação trafegada. É usado geralmente em comunicadores tais como Netscape Navigator e Internet Explorer junto com o protocolo TCP/IP visa garantir a segurança em canais de comunicação bidirecionais.

O SSL funciona na camada de transporte (abaixo da camada de aplicativo) e é independente dos protocolos de aplicativo utilizados [BUR 02].

Para atender os requisitos de segurança o SSL usa os seguintes componentes, segundo [GAR 99]:

- Algoritmos criptográficos para prover confidencialidade.
- Funções criptográficas de embaralhamento para prover integridade.
- Certificados de chave pública X.509 v3 para prover autenticação
- Mensagens assinadas criptograficamente para prover não-repúdio.

O SSL não é um simples protocolo, mas sim duas camadas de protocolos, como ilustrado na Figura 2.13 [STA 99].

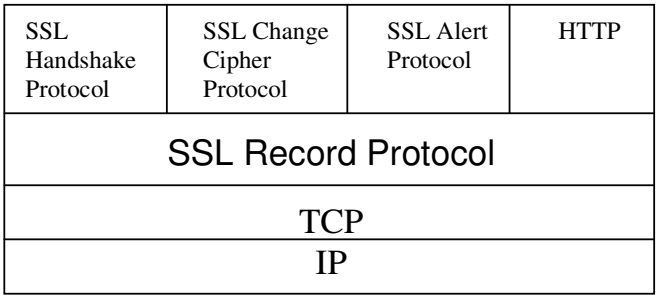

Figura 2.13: Camadas SSL

A camada SSL Record Protocol prove serviços de segurança básica para os protocolos da camada acima.

O protocolo HTTP da camada acima provê serviço de transferência para a interação web cliente/servidor (neste caso abordado somente o protocolo HTTP)

O Handshake, Change Cipher Spec e o Alert são usados na administração das transferências ocorridas entre protocolos e camadas do SSL.

2.7.4 IP Security - IPSec

O IPSec provê a capacidade de comunicação segura através de uma LAN, através de uma WAN privada e pública e através da Internet [STA 99], implementando esta segurança no nível IP garantindo autenticação, confidencialidade e exportação segura de chaves criptográficas.

Por exemplo, uma empresa pode utilizar-se da tecnologia IPSec para prover uma comunicação segura entre dois pontos distantes utilizando como meio de transmissão a Internet. O protocolo IPSec opera em dispositivos de rede, como um roteador ou firewall que conecta cada rede a outro ponto distante [STA 99]. O tráfego IP não seguro provindo da rede local LAN com destino à WAN é encriptado e compactado pelo dispositivo de rede que opera o IPSec, o qual o envia para o ponto WAN destino. Este descompacta e decripta o conteúdo recebido por meio de um dispositivo de rede daquele ponto contendo o protocolo IPSec. Estas operações são transparentes à estações de trabalho e à servidores da LAN [STA 99].

Sendo que o protocolo IPSec pode ser implementado em outros componentes inclusive em softwares de usuários, torna-se possível que tendo acesso discado à uma rede que utiliza o protocolo IPSec o usuário possa usufruir deste protocolo por meio de um software que o implemente.

2.7.4.1 Serviços IPSec

O IPSec habilita o sistema a selecionar protocolos e algoritmos de segurança e introduzir chaves de criptografia requeridas para serem usados pelo serviço.

Os serviços de segurança do IPSec se utilizam de dois protocolos para prover segurança:

- AH (Authentication Header): protocolo de autenticação designado pelo cabeçalho do protocolo.
- ESP (Encapsulating Security Payload): protocolo de encriptação e autenticação designado pelo formato dos pacotes para aquele protocolo.

Os dois protocolos AH e ESP do IPSec suportam 2 modos de uso:

- Modo transporte: provê segurança para camadas superiores tais como TCP, UDP que operam diretamente acima da pilha IP.

- Modo Túnel: neste modo o pacote IP é totalmente protegido, os campos AH e ESP são adicionados ao pacote IP formando um novo pacote IP com outro cabeçalho. O original inteiro, ou secreto, pacote viaja através de um "túnel" de um ponto de uma rede IP para outro; nenhum roteador ao longo do caminho está apto a examinar o cabeçalho IP secreto[STA 99].

2.8 Firewall

A tecnologia Firewall (barreira de fogo) tem como finalidade estabelecer regras de acesso de uma rede para outra, negando acesso à conexões não permitidas e monitorando conexões com acesso livre.

Muito utilizado por empresas o Firewall é implementado geralmente entre uma rede local (LAN) e uma rede pública (WAN) como a Internet. Os acessos externos à LAN e acessos da LAN à WAN são regulamentados, alguns negados, outros permitidos sob controle.

Infelizmente, muitas empresas consideram a tecnologia dos firewalls como sua única estratégia de segurança [GAR 99], mas esquecem que somente implementando-os para prover restrições ao acesso externo deixam desprovida de segurança a rede LAN contra os ataques internos, que geralmente são menos considerados, mas são os mais freqüentes e com graves conseqüências.

2.8.1 Técnicas de controle de acesso

Para prover controle de acesso a tecnologia Firewall utiliza-se de quatro técnicas gerais:

- Serviço de controle: controla os tipos de serviço que podem ser acessados externamente e internamente.
- Controle de direção: determina se um serviço pode ser iniciado ou permitido a partir de um acesso externo ou interno.
- Controle de usuário: controla o acesso à um serviço de acordo com o usuário que estiver tentando utilizá-lo. Serve tanto para usuários externos quanto para internos.

- Controle de comportamento: Controla a utilização dos serviços, ou seja, pode-se controlar o acesso à partes de um serviço. Por exemplo, podemos inibir formas de SPAM em um servidor de E-mail, inibir acesso à partes restritas de um servidor WEB, etc.

Outras funções devem ser implementadas para tornar um firewall seguro. Além do controle de acesso aos serviços, um firewal deve prover serviços de alarmes para informar invasões ou tentativas, auditagem para documentar historicamente os ataques, tradução de endereços internos para externo com a finalidade de abstrair a localização do usuário ao acesso externo, podem ser implementadas também tecnologias de tunelamento com a finalidade de criar uma rede privada (VPN) usando a tecnologia IPSec para prover segurança de acesso agregada à segurança do conteúdo da informação.

2.8.2 Limitações de um Firewall

A concepção de um Firewall a princípio pode deixar de englobar certas exigências de segurança, que devem ser completadas com outras tecnologias. Podemos enumerar algumas destas deficiências:

- Somente os acessos que passam através do firewall podem ser protegidos. Acessos provindos de meios internos não previstos fogem ao controle.
- A engenharia social, ou seja, a colaboração de um usuário interno à uma invasão externa, pode prover meios para que um invasor com conhecimento de senhas e formas de burlar o firewall obtido por informações de membros da empresa possa invadir um site através de um firewall sem grandes problemas.
- A transferência de vírus por meio de acesso permitido através do firewall é difícil de ser controlada, pois o tempo necessário para checar cada mensagem em busca de vírus eletrônico inviabilizaria a operação de um firewall. Esta detecção pode ser deixada a cargo de serviços internos especializados no recebimento destas mensagens.

2.8.3 Tipos de Firewall

Os Firewalls podem ser divididos comumente em três tipos:

2.8.3.1 Packet-Filtering Router

Um pacote recebido é roteado ao seu destino ou descartado de acordo com um conjunto de regras estabelecidas pelo firewall, sendo que estas regras são válidas tanto para os pacotes entrantes na rede quanto para os pacotes saintes.

As regras de filtragem são baseadas nos campos do protocolo TCP/IP os quais definem fonte e destino da informação, tipo de protocolo de transporte utilizado, TCP ou UDP e tipo de aplicação destes protocolos tais como TELNET ,SMTP, SNMP,etc.

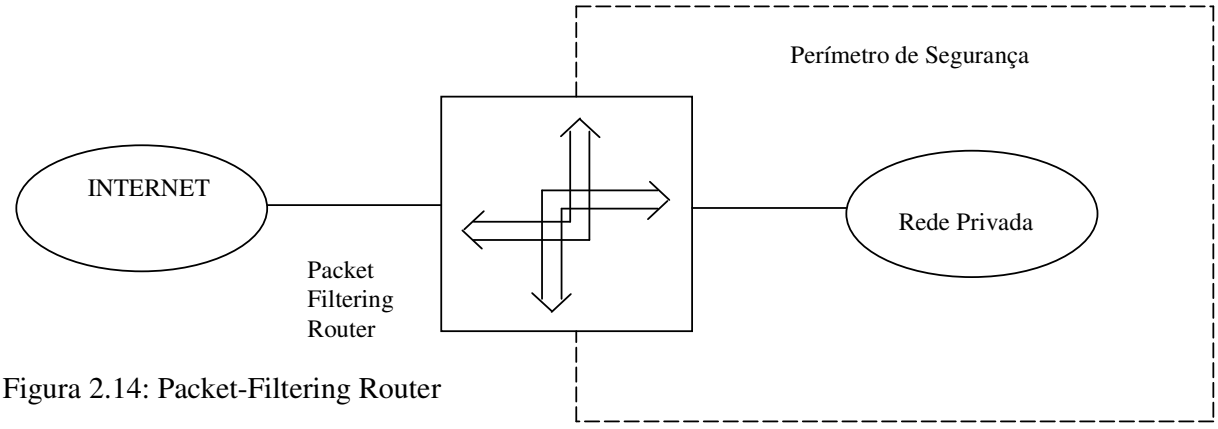

Figura 2.14: Packet-Filtering Router

2.8.3.2 Application-Level Gateway

Também chamado de servidor proxy, age como um retransmissor do tráfego no nível de aplicação[STA 99].

O usuário acessa o servidor proxy através de uma aplicação como TELNET ou FTP e informa o seu nome e destino requerido. O servidor proxy por sua vez valida o acesso através do nome do usuário e contata a aplicação destino e retransmite segmentos TCP contendo dados da aplicação entre os dois pontos. Se o servidor proxy

não implementa mecanismos para uma certa aplicação, sua comunicação não pode ser viabilizada através deste firewall.

O usuário pode estabelecer regras em um servidor proxy permitindo:

- acesso aos usuários somente à algumas aplicações
- acesso à aplicações somente por alguns usuários
- acesso somente à alguns usuários para utilização do servidor proxy.
- Acesso somente entrante ou sainte à algumas aplicações.

A configuração deste tipo de Firewall tende a ser mais simples, pois a tarefa de configurar as regras de aplicações e usuários permitidos é muito mais simples do que configurar as inúmeras possíveis combinações de permissão e negação do firewall Packet-Filtering Router.

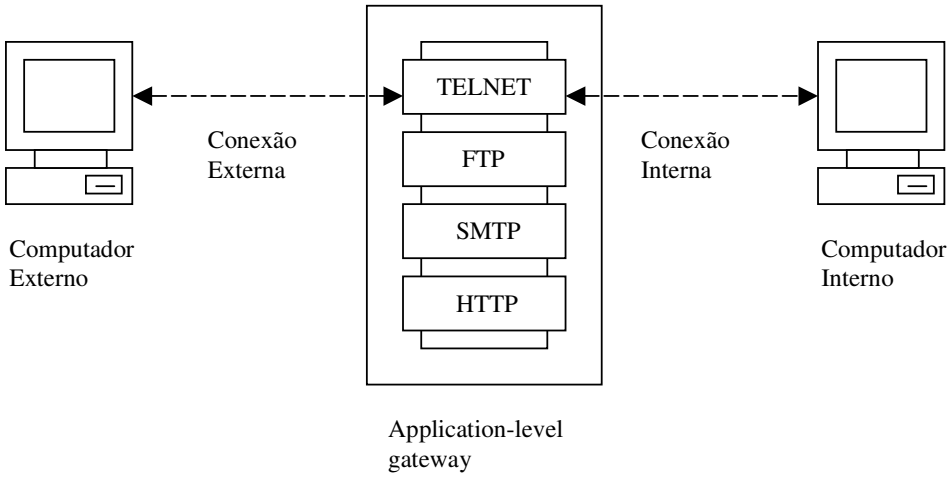

Figura 2.15:Application-Level Gateway

2.8.3.3 Circuit-Level Gateway

Este tipo de firewall não permite uma conexão TCP direta fim a fim. É configurada uma conexão entre o firewall e o usuário interno e outra entre o firewall e o destino.

O processo de comunicação se completa quando o firewall retransmite segmentos TCP de uma conexão a outra sem no entanto examinar o conteúdo desta comunicação. A função de segurança consiste de determinar quais conexões poderão ser permitidas [STA 99].

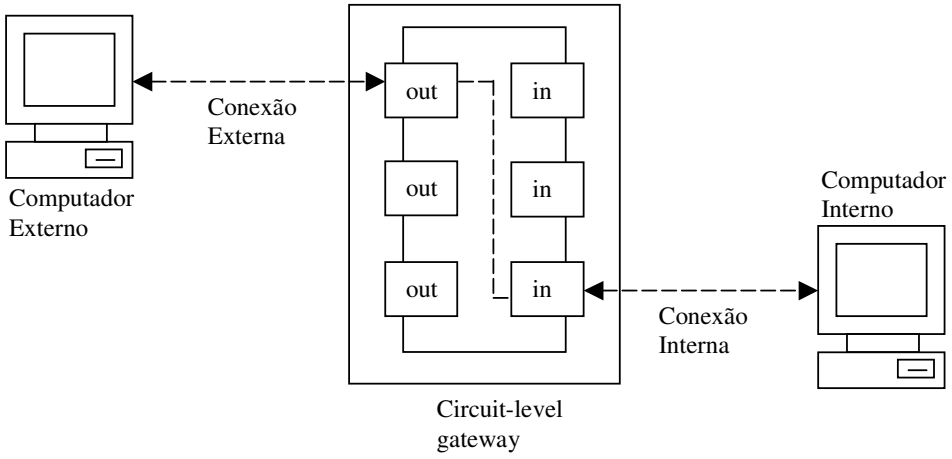

Figura 2.16: Circuit-Level Gateway

2.9 Pagamentos Digitais

"Os sistemas de pagamento digital provêem um meio de beneficiar alguém financeiramente não envolvendo transferência de objetos físicos de representação monetária tais como dinheiro papel/moeda, ouro, cheques, etc; e sim efetuando transferência eletrônica que realizem débito contra o pagador e crédito ao recebedor, é a capacidade de fazer pagamentos em bits em vez de em átomos "[GAR 99].

Atualmente a forma mais utilizada para beneficiar financeiramente transações eletrônicas via Internet é o cartão de crédito. O número do cartão de crédito a ser efetuado o débito é informado pelo consumidor ao comerciante numa transação via Internet em uma das seguintes formas:

- Off-line: depois do pedido ser feito via web, o consumidor entra em contato com o comerciante através de telefone, e-mail, fax, etc ;informando o número do cartão
- On-line com criptografia: o número do cartão de crédito é enviado ao comerciante pela Internet através de uma conexão segura criptografada.
- On-line sem criptografia: O consumidor envia o número do cartão de crédito através da Internet sem nenhuma segurança criptográfica implementada, passível de ser rastreado através de algum detetor de pacotes instalado na rede.

Dentre as três formas abordadas a forma On-line com criptografia é a mais segura e automatizada, mas a forma On-line sem criptografia é mais utilizada por ser mais facilmente implementada, mesmo não fornecendo a segurança necessária não tem sido alvo comum de fraudes.

A utilização do cartão de crédito em transações via Internet restringe um pouco o público consumidor. Não são todas pessoas no mundo que tem possibilidade de possuir um cartão de crédito pois envolvem custos adicionais e até abertura de contas bancárias, e também o uso de um cartão de crédito numa compra envolve a identificação do consumidor, que às vezes prefere o anonimato.

Tecnologias que possibilitem uma transação eletrônica com pagamento digital anônimo tem sido desenvolvidas, sendo aqui abordadas duas tecnologias.

2.9.1 DigiCash - Sistema de Pagamento Eletrônico

O DigiCash é um sistema de pagamento eletrônico desenvolvido pelo Dr. David Chaum, que é considerado como o inventor do dinheiro digital[GAR 99], e tem como finalidade proporcionar a cunhagem de moedas eletrônicas por um usuário.

O usuário instala o software DigiCash em sua máquina e se associa à uma instituição monetária que tenha permissão de cunhar e receber moedas digitais através do sistema DigCash. Deve ser efetuado um depósito bancário na instituição monetária a fim de prover saldo para cunhagem das moedas digitais. O usuário requisita a cunhagem de moedas digitais na instituição monetária. Estas são enviadas ao usuário para uma carteira eletrônica mantida em seu computador. Estas moedas digitais podem ser trocadas com comerciantes sem que o mesmo tenha conhecimento de sua origem. Para transformar dinheiro digital em dinheiro real o recebedor deve acessar a instituição financeira que garante o valor monetário físico do dinheiro digital.

2.9.2 Mondex – Sistema de Pagamento Eletrônico

Mondex não é um sistema de pagamento baseado na Internet, mas é um sistema de pagamento muito utilizado atualmente. O Mondex é um sistema fechado baseado em

um pequeno cartão inteligente, que teoricamente não pode ter seu projeto revertido, e além disso utiliza um protocolo secreto [GAR 99].

O cartão Mondex é carregado com informações eletrônicas que representam uma certa quantidade de dinheiro a partir de um dispositivo especial utilizando rede de comunicação ATM. O pagamento de uma conta é viabilizado com a transferência de saldo do cartão por um dispositivo existente no comerciante, o qual guarda este saldo em uma carteira eletrônica especialmente projetada.

2.10 Publicação

A disponibilização de informações tem sido facilitada pelas diversas tecnologias eletrônicas atualmente desenvolvidas. A disponibilização de documentos da forma que vem sendo efetuado através de órgãos expedidores como cartórios, não acompanha os progressos conquistados nos últimos anos.

Com a evolução tecnológica atual e com a abrangência que proporciona a Internet geograficamente, tornou-se viável a disponibilização de dados de maneira muito eficaz. O quesito segurança tem sido uma barreira tradicional ao uso da Internet, como meio viabilizador desta disponibilização eletrônica de dados.

O uso de tecnologias paralelas de comunicação, com controle rígido, proporcionaria um nível de confiança diferenciado à disponibilização destas informações, pois tornaria o acesso a este recurso controlado rigidamente por entidades governamentais ou privadas, responsáveis pelo acesso e pela integridade da informação circulada, estaríamos praticamente livres da anarquia que é a Internet, relativo à segurança e ao acesso. Mas nem sempre o que segue uma regulamentação rígida e controlada acaba se tornando popular como é o caso da Internet, com seus milhões de usuários e sua abrangência mundial.

O sucesso da implantação de um novo conceito, tal como cartório virtual, depende muito do alcance geográfico e social proporcionado, e também se deve levar em conta o fator financeiro que envolve o projeto, pois o uso de uma tecnologia popular é muito menos dispendiosa do que utilizar-se meios de comunicação de uso restrito, com onerosos custos de controle e manutenção. Paga-se entretanto o preço dos

contínuos cuidados com a segurança que exige a Internet, mas, nem os meios de acesso restrito fogem a este tipo de preocupação.

A disponibilização de recursos computacionais para o usuário final, para se ter sua utilização incentivada, deve contar com a elaboração de modos de acesso baseados em interfaces gráficas de fácil entendimento a pessoas de vários níveis sociais e culturais, contando com apoio de conceitos de ergonomia que exijam do usuário um mínimo de esforço na obtenção das informações.

Para o sucesso de um novo conceito tal como disponibilização de documentos eletrônicos, deve-se oferecer um diferencial encantador ao usuário em relação aos meios tradicionais utilizados anteriormente. A segurança, facilidade, rapidez e popularidade no acesso às informações, são os meios necessários para a viabilização efetiva de tal tecnologia.

2.10.1 Projeto Biblioteca Digital Brasileira

O projeto Biblioteca Digital Brasileira - BDB, propõe-se a integrar em um único portal os mais importantes repositórios de informação digital do país, de forma a permitir consultas simultâneas e unificadas aos conteúdos informacionais destes acervos[IBI 02].

O objetivo básico do projeto BDB é disponibilizar documentos eletrônicos que venham contribuir com o desenvolvimento de atividades técnicas , científicas, educacionais, produtivas, culturais, etc. Se utilizando da Internet como meio divulgador fornece um acesso facilitado à todos segmentos da sociedade inclusive divulgando informações culturais, artísticas, históricas, contribuindo para preservação de nossa identidade cultural.

O portal Internet da BDB proporcionará acesso aos vários acervos existentes de forma centralizada, sendo os dados oriundos de base de dados, documentos digitais e serviços de informação integrados de forma padronizada visando proporcionar a busca e obtenção de informações rápida e simplificada. Serão concebidos e integrados à BDB novos serviços de informação que venham atender demandas da sociedade

A integração dos vários acervos digitais será viabilizada através de indexadores virtuais criados a partir de metadados, que são formas de representação de conteúdo de

documentos eletrônicos. Esta base de indexadores viabilizará a busca de qualquer conteúdo que se encontre na base de informações de forma rápida e otimizada.

O sistema de busca do projeto BDB além de utilizar-se da base de indexadores do próprio portal, viabiliza também a integração com outros serviços de informação, na busca de informações que não estejam disponíveis no site centralizador. Esta integração automatizada é possível quando o serviço de informação utilizar o mesmo conjunto de protocolos do BDB, ou seja o protocolo Z39.50, largamente utilizado em todo mundo por produtores de bases de dados, redes de bibliotecas e serviços de intermediação.

Quando o serviço de informação não utilizar o protocolo Z39.50 a integração também será possível, porém não de forma automatizada.

O acesso ao BDB pelo usuário poderá ser feito através de computadores pessoais utilizando browsers, acessando um gateway ao protocolo Z39.50 e possibilitando uma busca integrada e simplificada na base de metadados e nos diferentes provedores de serviços que se utilizam do protocolo Z39.50.

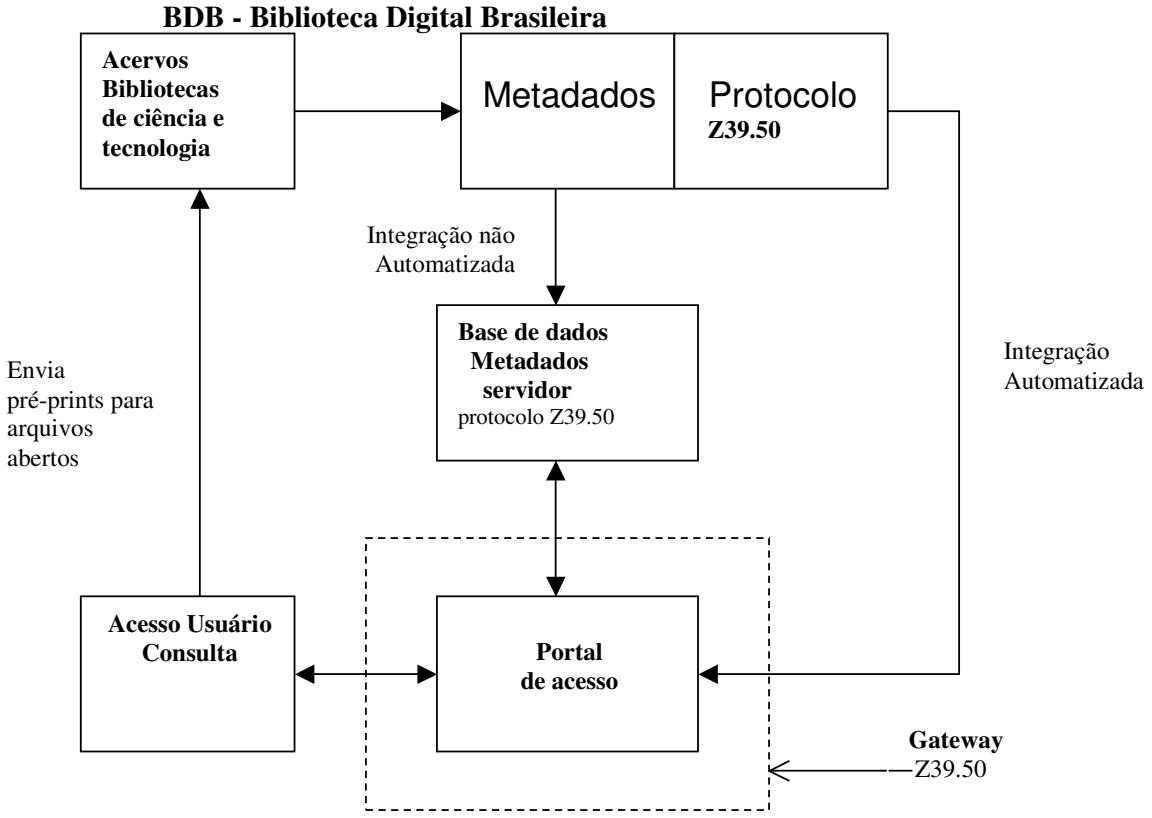

Figura 2.17: BDB Biblioteca Digital Brasileira

Os usuários terão ainda o papel de provedor de informações para acervos que permitirem tal operação, como os Arquivos Abertos de pré-prints, bases de teses e anais de congresso[IBI 02]. Esta submissão de informação à um acervo poderá ser feita pelo próprio usuário através do gateway de acesso, utilizando formulários eletrônicos, programas especializados e procedimentos de auto ajuda.

Para ser possível esta gama de integrações foram padronizadas várias tecnologias empregadas tais como:

a) Acesso dos usuários aos recursos da BDB: protocolo Z39.50;
b) Formato da base comum de metadados: Dublin Core, OpenArchives
c) Intercâmbio de documentos eletrônicos: XML
d) Padrão de digitalização de documentos: TIFF a 24 bits

A implantação de um projeto de biblioteca digital à nível de nacional, tal como a BDB exige conhecimento pleno das tecnologias aplicadas, regulamentação das divulgações e um projeto de divulgação nacional para que haja sucesso na implantação e uso do recurso disponibilizado.

2.10.2 Protocolo Criptográfico para Emissão de Certidões de Nascimento.

O Protocolo Criptográfico para Emissão de Certidões de Nascimento na Internet (ECN) apresentado por Laurentino Augusto Dantas em sua dissertação de Mestrado de Ciências da Computação da Universidade Federal de Santa Catarina no ano de 2001, foi concebido com a intenção de agilizar a obtenção da certidão de nascimento eliminando deslocamentos desnecessários do usuário e garantindo que seja emitida uma certidão de nascimento a cada novo cidadão.

O protocolo sugerido utiliza uma Central de Registro (CR), implementada através de um site Internet que será acessada pelo cartorário e por agentes responsáveis pelo registro de nascimento, comumente a maternidade.

A CR ficará sob responsabilidade do cartorário, que irá gerenciar o sistema e controlar o acesso, permitindo que apenas pessoas autorizadas consigam efetuar os registros de nascimentos[LAU 01].

Será responsabilidade da CR:

1. receber os registros dos Agentes Autorizados, verificar a validade das informações e garantir data e hora dos registros.
2. efetuar a liberação com autorização do Cartorário, verificar a validade das informações e garantir data e hora das liberações.
3. armazenar todas a informações, registros e liberações, de maneira segura e confiável, garantindo sempre a integridade das informações armazenadas.
4. garantir o acesso ao sistema apenas para pessoas autorizadas.

O acesso do agente autorizado e do cartorário à CR será efetuado utilizando-se a tecnologia de certificados digitais a fim de garantir a identidade dos envolvidos.

A autenticidade dos documentos eletrônicos trocados entre agente autorizado, CR e cartorário é viabilizada através de assinatura digital dos mesmos garantindo a procedência.

Para prover a autenticidade dos certificados digitais a serem utilizados, se fez necessário utilizar uma autoridade certificadora publicamente confiável.

Foram sugeridos três propostas de viabilização do projeto com vistas a facilitar uma possível implementação.

Na proposta seguindo o modelo atual o agente autorizado acessa o site da CR entrando com a declaração de nascido vivo e documentos dos pais dando início ao processo de registro do recém nascido..

Do lado do cartório o cartorário recebe dados para registros de nascimento a partir de um acesso à CR e segue os procedimentos convencionais para efetuar o registro.

A obtenção da certidão de nascimento é viabilizada junto ao cartório ao qual foi encaminhado o registro ou depende do encaminhamento da mesma ao agente autorizado para ser entregue aos pais

Esta proposta tende a viabilizar uma rápida implantação, pois não envolve mudanças profundas ao processo, garantindo o registro da criança sem o deslocamento do responsável pelo registro, mas a automatização do processo é parcial.

A proposta com um banco de dados em substituição ao Livro de Registro além de prover as facilidades da proposta acima, visa automatizar as operações de registro no que diz respeito ao armazenamento das certidões e dados agregados em base informatizada, sendo que após a efetivação do registro o cartorário emite a certidão e envia ao agente autorizado para ser disponibilizado aos pais.

O processo ainda não é totalmente automatizado, provê facilidades no armazenamento e restringe a possibilidade de duplicidade de registro.

A proposta com um banco de dados e emissão da certidão on-line se utiliza das facilidades das proposta acima e ainda fornece automatização total ao processo possibilitando que os pais possam receber a certidão de nascimento no próprio agente autorizado imediatamente após o registro, sendo assinada pela própria CR, ficando o cartório responsável somente em manter o sistema e controlar quem pode efetuar o registro.

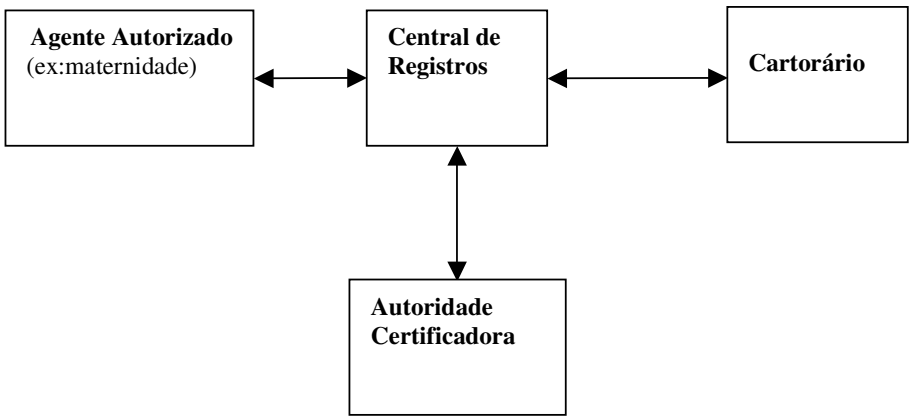

Figura 2.18: Representação simplificada genérica das três propostas do ECN.

"O presente projeto foi apresentado na Fenasoft nos anos de 2000 e 2001, e demonstrou ser um trabalho de grande aceitação pela opinião pública, levando em consideração o entusiasmo das pessoas que visitaram o *stand* da Universidade Federal de Santa Catarina(onde um protótipo estava exposto). A Emissão de Certidão de

Nascimento através da Internet teve grande atenção da imprensa, tendo sido citado em reportagens de diversos jornais e revistas de diferente áreas.

A definição de um protocolo seguro para emissão de certidão de nascimentos através da Internet, pode ser o primeiro passo de um grande processo de modernização dos serviços dos cartórios, desde que os estudos não sejam encerrados e novos trabalhos sejam iniciados[LAU 01].

3 SISTEMA DE DISPONIBILIZAÇÃO DE DOCUMENTOS LEGAIS

3.1 Introdução

Os progressos tecnológicos alcançados nos últimos tempos regulamentando a validade de documentos eletrônicos e identidade digital deram respaldo ao desenvolvimento de novas técnicas que possibilitam a desburocratização.

A disponibilização de documentos legais de forma eletrônica, de modo descentralizada, rápida, íntegra e segura ao usuário gera uma otimização de procedimentos tanto no lado dos órgãos disponibilizadores de documentos, quanto no lado do usuário que necessita de agilidade para efetivar transações.

Analisando brevemente o modo tradicional de disponibilização de documentos, em órgãos tais como cartórios, notamos que temos um respaldo oficial na guarda e obtenção de documentos tradicionalmente confiável.

O sistema de disponibilização de documentos legais apresentado neste trabalho preserva a função do órgão disponibilizador de armazenar e disponibilizar documentos diretamente ao usuário, mas contando agora com mecanismos de disponibilização eletrônica direta, podendo garantir a autenticidade como na forma tradicional, sem necessidade do usuário comparecer ao órgão disponibilizador.

3.2 Considerações

A entidade Órgão Disponibilizador de Documentos (ODD), mencionada na introdução deste capítulo refere-se à qualquer entidade geradora e/ou disponibilizadora de documentos à usuários, as quais pode-se relacionar algumas que tenham afinidade de integração com o sistema proposto nesta dissertação:

- Cartórios em geral.
- Órgãos de Saúde.
- Universidades.
- Órgãos governamentais.
- Área de pesquisa.

Entre as funções relativas ao ODD relaciona-se:

- Manter site Internet e sistema de disponibilização de documentos com acesso à usuários e RDDE.
- Cumprir regras relativo ao funcionamento do sistema estabelecidas pela RDDE.

A Rede de Disponibilização de Documentos Eletrônicos (RDDE) é a entidade responsável por intermediar as operações de visualização e disponibilização de documentos entre usuários e ODDs.

Entre as funções relativas à RDDE relaciona-se

- Manter site Internet e sistema de disponibilização de documentos com acesso à usuários e ODDs
- Coordenar operação dos ODDs por meio de regras estabelecidas.

3.3 Síntese de funcionamento da proposta

O Sistema de Disponibilização de Documentos Legais de forma eletrônica ou seja o SDDL, sugerido nesta proposta envolve basicamente três componentes:

- O usuário interessado na obtenção do documento autenticado pelo ODD.
- O ODD conveniado à rede de disponibilização de documentos eletrônicos.
- A Rede de Disponibilização de Documentos Eletrônicos (RDDE), que irá intermediar o acesso entre o usuário e os ODDs conveniados, no processo de obtenção de documentos.

O usuário interessado em ingressar na RDDE dirige-se à um ODD conveniado a fim de efetuar seu cadastro.

Ao usuário é requerido a apresentação de documentos pertinentes ao cadastro de novos usuários. Caso o usuário possua um certificado digital de uma Autoridade Certificadora válida que o identifique, seu acesso futuro ao sistema será viabilizado através do mesmo, caso contrário será utilizado o método tradicional, usuário/senha.

Após a efetivação de seu ingresso na RDDE esta disseminará a informação de cadastro para toda rede de ODDs conveniados.

Os ODDs conveniados ao receberem esta informação de cadastro, de forma automatizada efetuarão a associação local deste usuário com a RDDE.

A partir desta associação se o ODD tiver documentos relativos ao usuário, repassará ao site da RDDE de forma automatizada informações de documentos deste usuário, gerando uma base centralizada na RDDE de informações de documentos/ODD/usuário.

O usuário através do acesso somente à RDDE, obterá uma visão global de seus documentos em toda rede de ODDs conveniados.

Na necessidade de obtenção de um documento cuja informação de localização foi obtida através da RDDE, o acesso do usuário será encaminhado pelo site da RDDE ao ODD que possui o documento a ser disponibilizado. Caso o documento já esteja disponível na base de distribuição do ODD, sua disponibilização será feita de forma transparente e imediata, caso contrário o usuário receberá informação sobre prazo a ser disponibilizado, pois dependerá da digitalização de documentos existentes em meio físico. A Figura 3.1 apresenta o fluxo de funcionamento do SDDL**.**

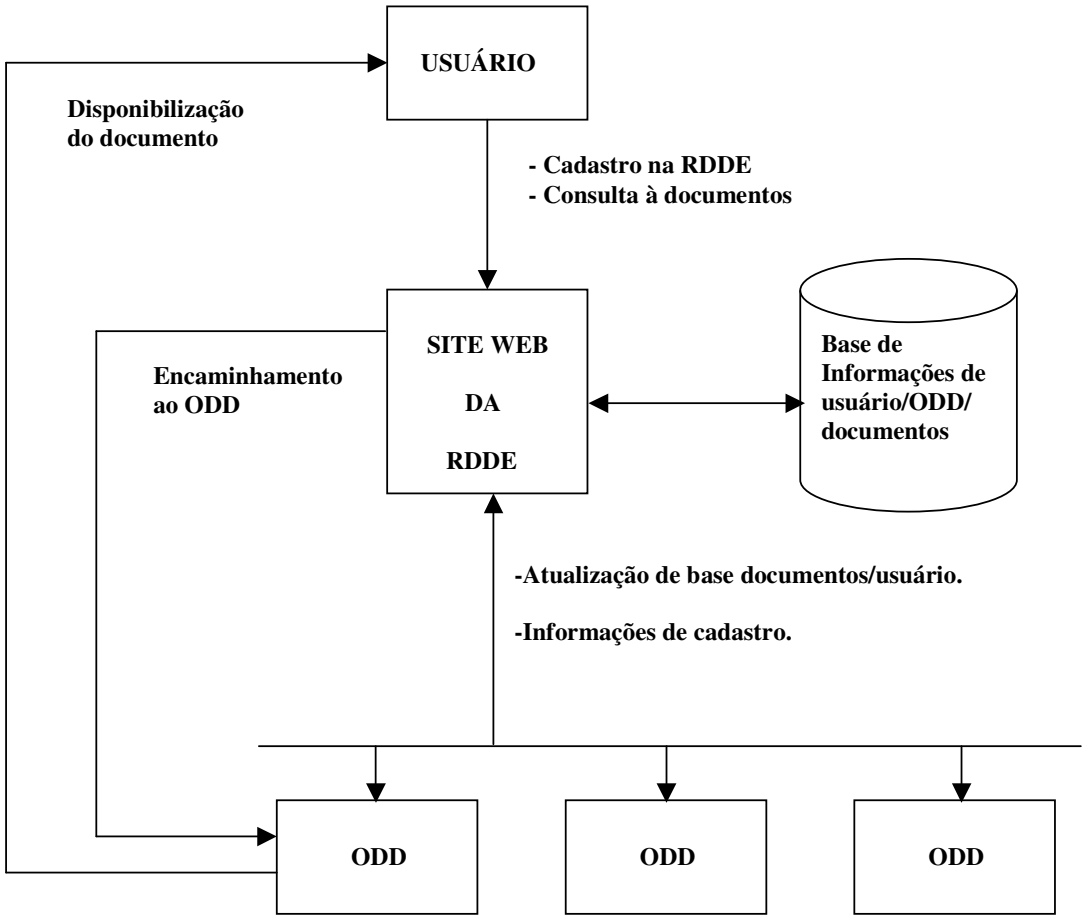

Figura 3.1: Disponibilização de documentos eletrônicos (RDDE)

A autenticação do documento a ser disponibilizado ao usuário pelo ODD será realizada com base nos mecanismos de assinatura digital abordados neste trabalho ou através de impressão local ao usuário com possibilidade de visualizar dados do usuário e imagem do documento diretamente através de acesso ao ODD detentor do documento, em prazo limitado acordado pelo usuário no processo de disponibilização.

Documentos produzidos originalmente de forma eletrônica deverão obrigatoriamente compor a base de documentos disponibilizados do ODD, pois agilizam o processo de disponibilização, não onerando de forma demasiada os recursos de armazenamento.

3.4 Detalhamento da proposta

As operações a serem realizadas pelo sistema proposto podem ser divididas em duas partes, seguindo a lógica usual de operação.

Serão detalhadas a nível de entendimento prévio as operações de:

- Ingresso do usuário na RDDE.
- Disponibilização de documentos legais ao usuário.

3.4.1 Ingresso na Rede de Disponibilização de Documentos Eletrônicos

O ingresso do usuário na RDDE envolve operações a serem realizadas no site da RDDE e nos ODDs conveniados.

Ao ser efetuado um cadastro de novo usuário na RDDE, estas informações cadastrais são repassadas aos ODDs conveniados, onde caso tenham documentos para este usuário realizam a associação de cadastro RDDE com cadastro interno e retornam à RDDE estas informações.

Passos a serem realizados:

- O usuário interessado dirige-se à um ODD conveniado responsável pelo cadastro de novos usuários na RDDE.

- A pedido do usuário, o operador responsável pelo cadastro de usuários na RDDE acessa a Interface de Cadastro de Usuários – ICU, do site Web da RDDE na área de cadastro de novos usuários.
- Apresenta seu certificado digital para ser reconhecido como autorizado a efetuar o cadastro. Caso a operação de identificação do operador ocorra com sucesso é disponibilizada uma tela de cadastro de novos usuários.
- O operador requer documentos do usuário a efetuar o cadastro.
- Insere dados do usuário no cadastro de usuários da RDDE.
- Caso o usuário tenha ou queira utilizar seu certificado digital para acesso ao sistema, viabiliza sua utilização, caso contrário proporciona cadastro de mecanismo tradicional de acesso.
- Informa políticas de uso da RDDE.
- Recolhe taxa monetária de uso do recurso, caso estabelecida por órgãos reguladores.
- O Serviço de Disseminação de Informações Cadastrais chamado SDIC a existir no site da RDDE exporta os novos dados cadastrais aos ODDs conveniados.
- Do lado do ODD um serviço parceiro do SDIC, o Serviço Receptor de Informações Cadastrais - SRIC, atualiza informações cadastrais que serão integradas através de um serviço chamado INTEGRADOR nas bases do ODD.
- Após terem sido integradas, caso o usuário seja cadastrado e tenha documentos no ODD, as informações de documentos por usuário serão exportadas à RDDE através do Serviço de Exportação de Informações - SEI do ODD.
- Estas informações de documentos por usuário exportadas pelo ODD à RDDE serão atualizadas pelo Serviço de Importação de Informações - SII na tabela de usuários / ODD / documentos, a qual possibilitará uma visão total de todos os documentos de um usuário em toda rede conveniada de ODDs.
- No ODD após a integração de um usuário existente à RDDE serão digitalizados, e armazenados em base de documentos digitalizados, tipos de documentos pré estabelecidos por órgão reguladores, a fim de ficarem disponíveis imediatamente ao usuário, como forma de incentivo ao uso do recurso de disponibilização de documentos eletrônicos.

A Figura 3.2 representa Ingresso do usuário na Rede de Disponibilização de Documentos Eletrônicos – RDDE.

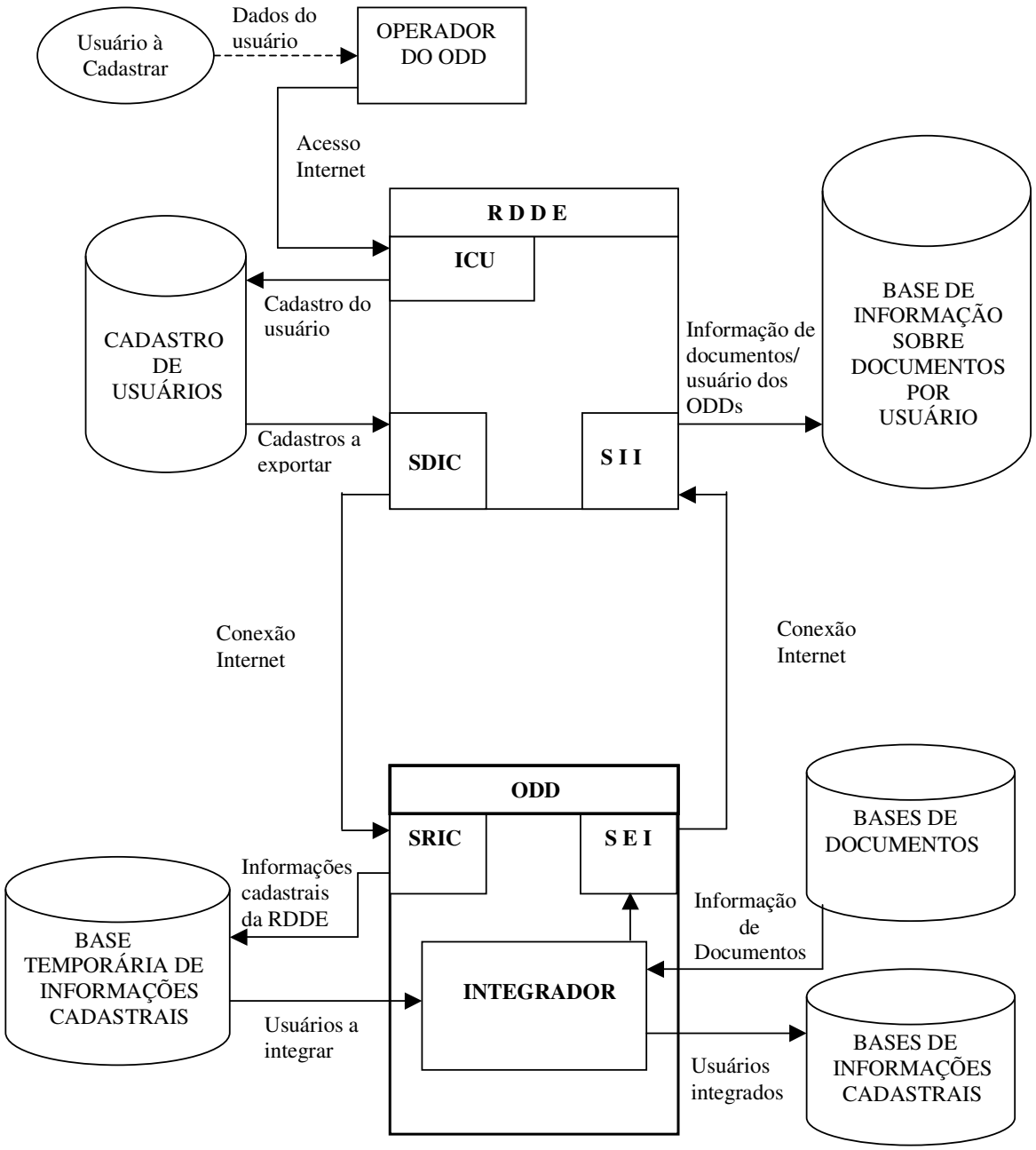

Figura 3.2: Fluxograma de ingresso do usuário na RDDE

3.4.2 Disponibilização de Documentos Legais ao usuário

A disponibilização de documentos legais ao usuário é viabilizada por meio do acesso à área de disponibilização de documentos da RDDE, que encaminha o acesso do usuário ao ODD detentor do documento, o qual disponibiliza imediatamente o documento ou agenda a disponibilização.

Passos a serem realizados:

- O usuário acessa via Internet o site da RDDE na área de disponibilização de documentos eletrônicos interagindo com a interface de Consulta e Encaminhamento para disponibilização - CED.
- Informa seu código de usuário ou apresenta seu certificado digital.
- Informa sua senha de acesso ou valida seu acesso com sua chave privada relativa ao seu certificado digital.
- Caso sua senha seja válida ou a operação de seu certificado digital ocorra com sucesso, disponibiliza uma visão em tela gráfica de todos os seus documentos na rede de ODDs conveniados.
- Caso escolha algum documento a ser disponibilizado, seu acesso será direcionado ao ODD detentor do documento selecionado, onde sua requisição será processada pelo Serviço de Disponibilização de Documentos – SDD e pelo Serviço de Obtenção Direta de Documentos SODD.
- Se o ODD tiver o documento disponível, digitalizado em sua base de documentos digitalizados para este usuário, requer definição do tempo de validade da autenticidade do documento a ser emitido e propicia formas ao usuário de pagamento monetário pelo uso do recurso e caso seja realizada com sucesso a transação financeira, disponibiliza ao usuário a forma de obtenção imediata do documento em forma impressa ou eletrônica através do Serviço de Obtenção Direta de Documentos - SODD.
- Se o ODD não tiver o documento disponível em sua base de documentos digitalizados, informa o prazo de disponibilização. Para que seja agendada a real disponibilização do documento, ao usuário é requerido a definição do tempo de

validade da autenticidade do documento a ser emitido e o acerto da transação financeira para propiciar a sua obtenção direta em prazo previsto.

- No caso de documentos à disponibilizar em prazo previsto, após a efetivação da transação financeira é fornecido ao usuário um código de acesso à disponibilização direta do documento a ser requerido no acesso do usuário ao serviço SODD.

Formas de disponibilização do documento ao usuário

Forma eletrônica.

Caso o usuário queira obter o documento em forma eletrônica o ODD viabiliza uma forma de transferência do documento assinado digitalmente ao usuário, utilizando um certificado de tempo limitado, segundo sua escolha realizada na operação de pedido de disponibilização.

Forma Impressa.

Caso o usuário prefira a impressão em papel, o ODD viabiliza uma interface de impressão, através da qual o documento é impresso no dispositivo de impressão do usuário, apresentado com segurança de marca d'água e no seu final um código de comprovação de autenticidade do documento a ser viabilizada por meio de um acesso ao site Web do ODD emissor do documento.

Verificação de autenticidade do documento disponibilizado

A fim de proteger o ODD quanto aos custos de armazenamento dos documentos de seus usuários por período indeterminado, os documentos a serem disponibilizados através da RDDE deverão ter seu prazo de verificação de autenticidade e validade limitados.

Quando da disponibilização do documento ao usuário é negociado o prazo de validade da verificação de autenticidade.

Se a disponibilização do documento ao usuário for feita de forma impressa, em seu dispositivo de impressão de seu computador pessoal, ao final da impressão é impresso um código de verificação de autenticidade.

Este código serve para acesso ao site do ODD para verificação de autenticidade do documento, por prazo limitado conforme acordado.

Acessando o site do ODD na área de Verificacão de Autenticidade de Documentos – VAD, de posse do código de autenticidade, o usuário ou órgão interessado obterá informações sobre o usuário a qual o documento pertence e a visão íntegra do documento digitalizado pelo ODD, com vistas a comparar seu conteúdo dando maior aval ao documento impresso apresentado pelo usuário.

Se o documento for disponibilizado através de transferência do mesmo digitalizado e assinado digitalmente pelo ODD, esta assinatura digital será realizada utilizando-se dados de um certificado digital com prazo de validade limitado, ou seja a validade de verificação de autenticidade do documento será propiciada diretamente ao usuário efetuando a validação da assinatura, não envolvendo acesso ao ODD emissor do documento.

Caso o certificado utilizado como base para assinatura do documento tiver seu prazo de validade expirado, a verificação de autenticidade do documento será inviabilizada, tendo que ser realizada outra transação de disponibilização do documento a partir de site da RDDE.

A Figura 3.3 representa a Disponibilização de Documentos Legais ao usuário.

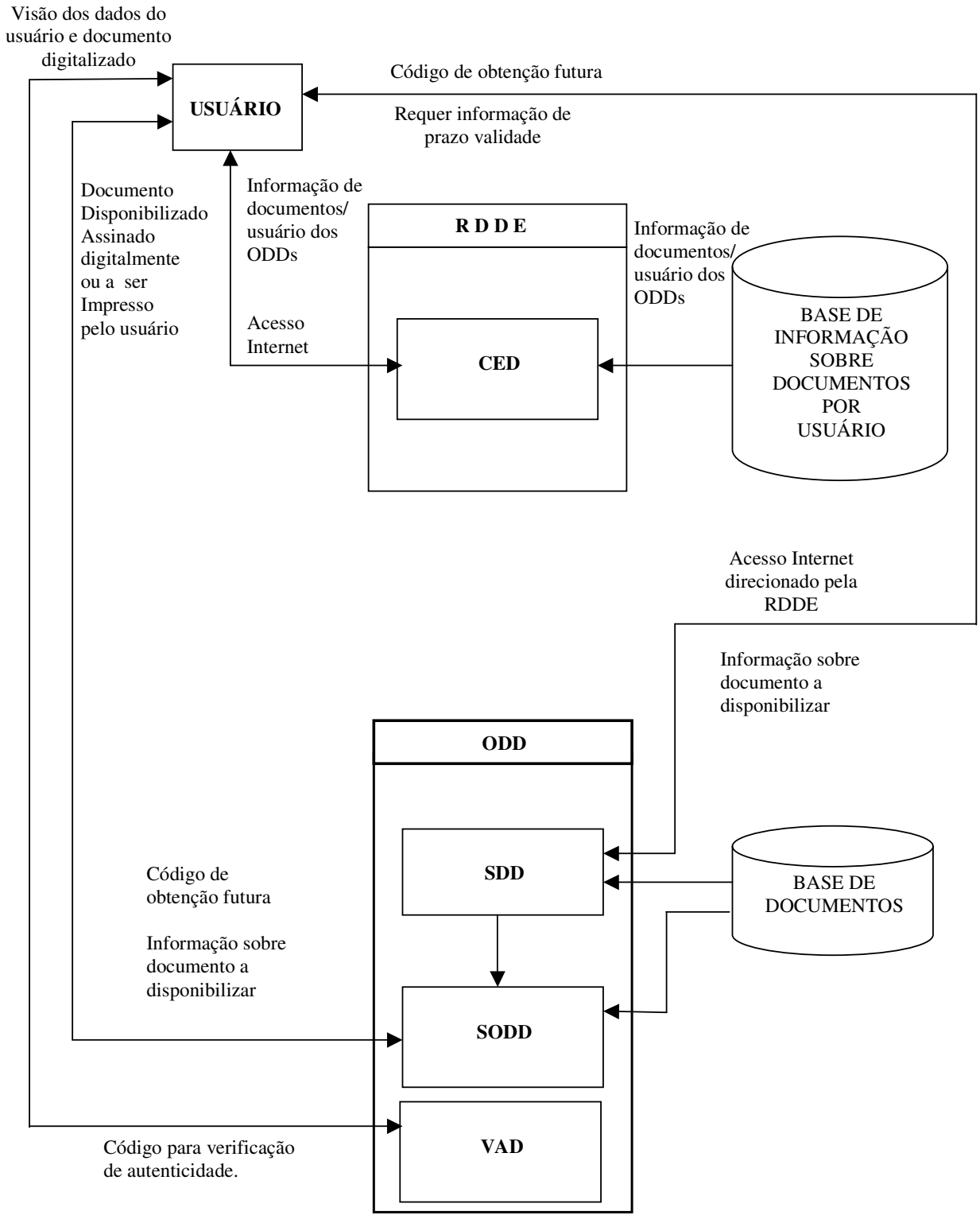

Figura 3.3: Fluxograma de disponibilização de documentos legais.

4 PROCEDIMENTOS METODOLÓGICOS

4.1 Arquitetura do Sistema

O sistema de disponibilização de documentos legais – SDDL, apresenta um diferencial em relação ao método tradicional no que diz respeito à facilidade de localização e obtenção de documentos requeridos.

O site da Rede de Disponibilização de documentos Eletrônicos (RDDE), concebido neste trabalho tem a função de centralizar os acessos dos usuários à vários órgãos de disponibilização de documentos, fornecer uma visão de seus documentos existentes nestes órgãos e encaminhar o usuário na operação de disponibilização.

A forma tradicional de disponibilização de documentos muitas vezes exige o deslocamento do usuário ao ODD e conhecimento exato da localização de documentos relativos a ele nos vários ODDs.

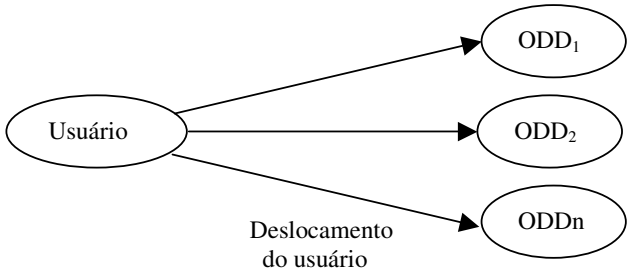

Figura 4.1: Modo tradicional de localização e disponibilização de documentos legais.

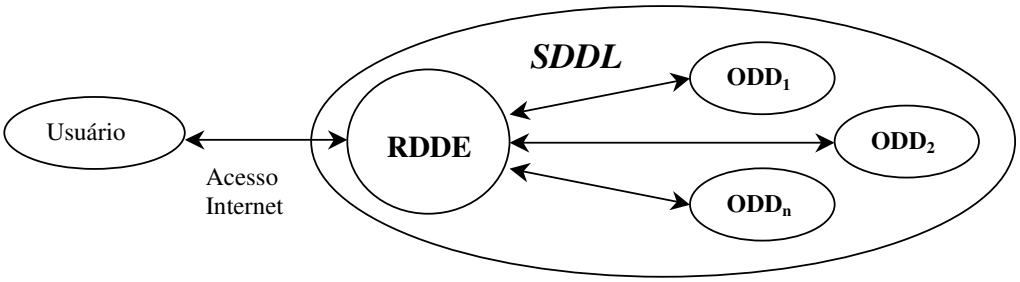

Figura 4.2: Sistema de Disponibilização de Documentos Legais - SDDL

O site da RDDE para cumprir o propósito basicamente deve ser composto de servidor de acesso, armazenamento de dados, e aplicação, sendo hospedeiro de serviços integrantes do SDDL, os quais irão interagir direta ou indiretamente com serviços do parceiros a existirem nos ODDs.

Além das funções técnicas que viabilizam o funcionamento do SDDL, os administradores da RDDE deverão estabelecer regras que regulamentem a utilização do SDDL pelos usuários e ODDs no que diz respeito ao acesso, prazo de disponibilização de documentos e outros requisitos necessários solicitados pela RDDE.

Os ODDs por sua vez implementarão os serviços parceiros componentes do SDDL que viabilizarão a interação com a RDDE e atenderão os requisitos de funcionamento impostos pelos administradores da RDDE visando proporcionar pleno sincronismo de atividade do SDDL.

4.1.1 Ingresso no SDDL e atualização de informações.

A concepção do SDDL teve como foco principal o benefício ao usuário final, fornecendo facilidades de acesso e obtenção de documentos relativos à sua pessoa.

O ingresso inicial de um utilizador em um determinado sistema utilizando a Internet como meio de acesso remoto, sem um prévio contato físico do utilizador com o órgão responsável pelo sistema, torna esta ligação entre utilizador/sistema possuidora de pontos frágeis no que diz respeito à garantia de autenticidade da identidade do utilizador e veracidade das informações cadastrais informadas.

Mesmo que o usuário seja utilizador do recurso de identidade digital, que garante a validade de sua assinatura digital temos o problema da perda de sigilo da chave privada, componente este integrante responsável pela viabilização do recurso de identidade digital tratado no capítulo 2, o que poderia proporcionar o cadastro fraudulento de um utilizador em um determinado sistema, obtendo assim informações particulares confidenciais e/ou onerando financeiramente e comprometendo o autêntico proprietário da identidade digital em questão.

A operação de ingresso de um usuário no SDDL visando garantir sua identificação idônea e informação legítima de dados cadastrais, foi concebida utilizando um órgão responsável por cadastro de usuários na RDDE.

O usuário interessado em seu ingresso como utilizador do SDDL dirige-se a um órgão responsável e credenciado pelo cadastro de usuários na RDDE com posse de documentos necessários, requerendo seu ingresso na RDDE com a utilização do recurso de identidade digital, caso tenha e queira utilizar. Assim fica o órgão responsável pela entrada correta de dados relativos ao cadastro do usuário, baseado em documentos apresentados.

Desta forma o ingresso do usuário no SDDL se torna muito mais confiável, pois há garantia da identidade e correta entrada de dados cadastrais.

Utilizando-se um órgão responsável por cadastro de usuários temos também a facilidade de viabilização de cobrança de taxas monetárias de ingresso ao sistema, caso haja, e o fornecimento direto de informações sobre utilização do sistema e resolução de dúvidas do usuário.

A interação entre a RDDE e ODDs, tanto a disseminação de cadastros quanto a atualização de informações por usuário na RDDE, ocorre de forma automática em intervalos de tempo pré definidos a serem executados pelos serviços de atualização remota de informações tais como o SDIC/SRIC e SEI/SII, sendo que o contato entre RDDE e ODDs ocorre utilizando-se a Internet como meio de comunicação através de protocolo seguro atualmente existente e aplicado em transações comerciais e financeiras, visando coibir ações tais como visualização, alteração de informações e acesso indevido ao sistema.

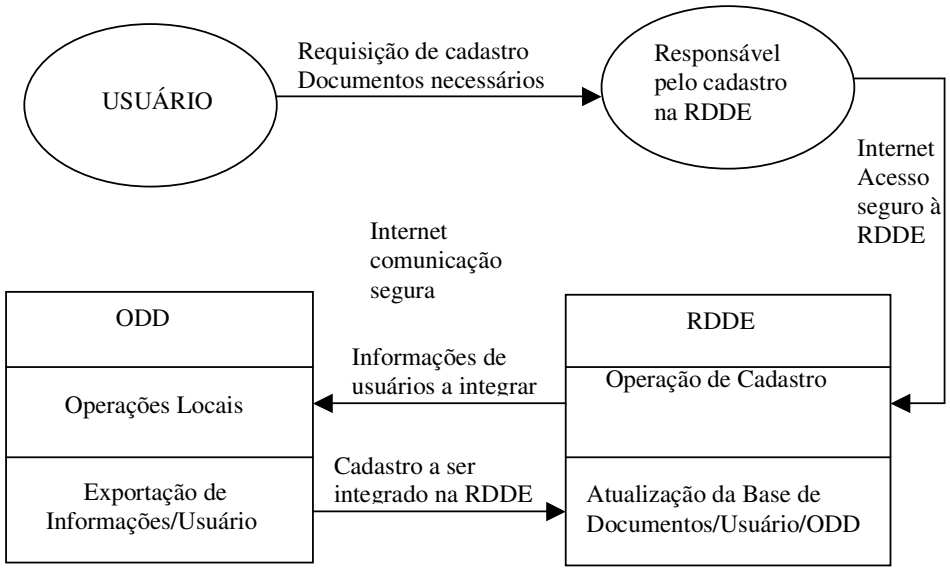

Figura 4.3: Ingresso e atualização de informações

4.1.2 Disponibilização de documentos.

A utilização de um site centralizador de acessos como discutido no item anterior, provê uma visão centralizada de informações de documentos por ODD, mas fica restrito sua operação à localização e encaminhamento do acesso do usuário ao ODD detentor do documento solicitado, ou seja, após o usuário selecionar o documento a disponibilizar sua interação com o SDDL passará a ser atendida pelo ODD que disponibilizará o documento requerido.

A partir daí a RDDE somente receberá alertas administrativos caso o procedimento de disponibilização venha ferir as regras estabelecidas para o funcionamento do SDDL.

O ODD por sua vez não proverá recursos para acesso originado diretamente pelo usuário em operações de localização e disponibilização de documentos, ficando o usuário obrigado a acessar o site da RDDE para efetuar estas operações. Com isso teremos um controle centralizado de utilização do SDDL por parte dos usuários.

A operação direta de disponibilização realizada pelo ODD somente será realizada com a utilização do código de obtenção futura fornecido pela ODD, caso a disponibilização tenha que ocorrer em prazo determinado devido a ausência do documento digitalizado nas bases do ODD no ato do pedido de disponibilização encaminhado pela RDDE.

Outra forma de acesso direto do usuário ao ODD ocorre quando da disponibilização do documento em forma impressa, com código de verificação de validade por tempo determinado impresso ao final da impressão. De posse deste código o usuário dentro de um prazo pré determinado acessa diretamente o ODD, para verificar a autenticidade do documento disponibilizado de forma impressa.

Caso as operações de disponibilização em prazo determinado e verificação de autenticidade do documento realizadas no ODD venham causar imprevistos incômodos ao usuário previstos nas normas administrativas, são emitidos alertas à administração da RDDE visando manter um nível de operação satisfatória do SDDL.

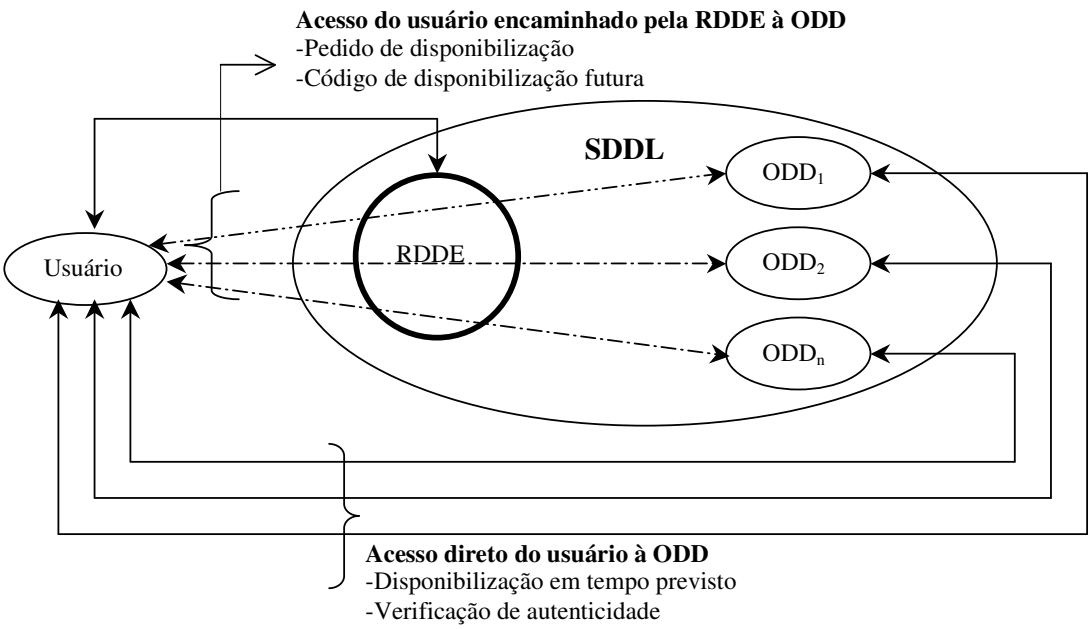

Figura 4.4: Disponibilização e verificação de autenticidade de documentos

As funções de ingresso do usuário e disponibilização de documentos para serem viabilizadas de forma eficaz dependem grandemente da operação interna dos ODDs conveniados ao SDDL no que diz respeito a:

- Manter operacional a estrutura de acesso ao sistema e comunicação com o site da RDDE.
- Manter o sistema computacional provedor do SDDL ativo e funcional.
- Resolver divergências na associação de cadastro RDDE/ODDs.
- Digitalizar documentos requeridos em prazo hábil.

O site da RDDE por sua vez deve contar com uma estrutura administrativa que venha garantir o funcionamento de todo o SDDL, no que diz respeito tanto às regras estipuladas para interação entre Usuário – RDDE – ODD, quanto aos procedimentos técnicos de operação do SDDL, sendo citados abaixo algumas preocupações.

- Manter operacional a estrutura de acesso ao sistema e comunicação com os ODDs e usuários.
- Manter o sistema computacional provedor do SDDL ativo e funcional.

- Prover alterações na concepção do sistema e/ou manutenções no projeto, repassando estas atualizações de forma automatizada aos ODDs.
- Integrar novos ODDs ao sistema.

4.2 Funcionalidades

A centralização de informações com acesso facilitado aos interessados provê recursos para desburocratização em diversos segmentos da sociedade.

O Sistema de Disponibilização de Documentos Legais de forma eletrônica abordado neste trabalho visa proporcionar a viabilização desta centralização de informações, provendo conhecimento centralizado e disponibilização descentralizada de informações, utilizando-se da infra estrutura da Internet para comunicação entre interessados e provedores.

Quesitos segurança de acesso e sigilo da informação disponibilizada são aplicados baseando-se em leis de apoio que regem a validade e autenticidade da informação eletrônica.

Os fatos acima mencionados dão respaldo à utilização do SDDL em diversos segmentos que tenham necessidade de disponibilizar documentos à interessados de forma centralizada e segura, ou seja, pode-se construir redes de disponibilização de documentos em ambientes industriais, comerciais, universidades, etc; baseando-se no SDDL.

Sendo que as tecnologias de segurança e disponibilização de informações aplicadas são de domínio público, a participação de um disponibilizador de informações como membro da RDDE torna-se facilitada, dependendo somente de acordos de colaboração pré estabelecidos e adequação do ambiente tecnológico do disponibilizador de documentos aos requisitos da RDDE.

Assim sendo, podemos ter mesmo disponibilizadores domésticos envolvidos na elaboração de uma rede de disponibilização de documentos.

Abaixo relaciona-se alguns possíveis órgãos de disponibilização de documentos que venham compor RDDE com afinidade entre si:

- Cartórios Cíveis, de Registro, de Notas: disponibilizando aos cidadãos e órgãos interessados documentos emitidos pelo cartório, comprovando autenticidade do mesmo.
- Universidades: na disponibilização de informações pertinentes aos alunos com respaldo do órgão, disponibilização de artigos técnicos, transferência de informações sigilosas de forma autêntica.
- Serviços de saúde: na centralização e disponibilização de históricos médicos de pacientes, abrangendo diversas especialidades e profissionais de saúde no qual se envolveu o paciente em tratamento de saúde, atendendo os requisitos de segurança da informação necessários.
- Governo público: centralizando informações sobre posses e pendências do usuário em diversos órgãos públicos governamentais.
- No meio industrial e comercial: centralizando e disponibilizando informação de projetos internos e externos à entidade de forma sigilosa ou não.
- No meio científico: visando compartilhar componentes de estudo científico desenvolvido em diversas entidades científicas, visando proporcionar um trabalho colaborativo entre pesquisadores, de forma sigilosa ou não.

4.3 Tecnologias empregadas

O quesito segurança é de suma importância para o funcionamento do SDDL, sendo que para prover confiabilidade à tal projeto, especial atenção dever ser dada à segurança e autenticidade da informação disponibilizada, ao acesso ao sistema e à segurança da informação trafegada entre os envolvidos no processo. Os itens 4.3.1, 4.3.2 e 4.3.3 deste capítulo tratam da segurança descrita acima.

O armazenamento de dados requerido pelo sistema é exposto no item 4.3.4 deste mesmo capítulo, sendo abordadas tecnologias a serem envolvidas.

4.3.1 Acesso ao SDDL

A utilização de controle de acesso baseado em certificados digitais obtidos de Autoridades certificadoras confiáveis é a forma nativa de acesso ao sistema abordado,

porém em algumas situações poderão ser utilizados métodos tradicionais de controle de acesso de acesso tal como usuário/senha.

A possibilidade de uso de métodos tradicionais de controle de acesso ao sistema se deve ao fato que nem sempre o usuário dispõe do recurso de identidade digital e na falta de necessidade de controle rígido de acesso à alguns serviços do SDDL.

O acesso à operação de cadastro de usuários na RDDE (serviço ICU) realizada por operadores dos ODDs, deve obrigatoriamente ser efetuado utilizando-se o recurso de identidade digital , a fim de garantir maior segurança ao processo de cadastro. Mas o cadastro do usuário propriamente dito pode ser realizado utilizando-se identidade digital ou mecanismo tradicional como meio de acesso futuro, visando não inviabilizar o cadastro para usuários que não possuam o recurso de identidade digital.

O acesso do usuário ao sistema em operações de disponibilização de documentos (serviço CED), pode ser efetuado através do uso de certificados digitais ou mecanismo usuário/senha, de acordo com que foi estabelecido na operação de cadastro do usuário na RDDE.

O acesso de operadores dos ODDs conveniados à operações rotineiras do próprio ODD (serviços SAM, DIGIT e cadastros) a serem abordadas no item 4.4, foi concebido neste trabalho com o uso de mecanismos tradicionais de usuário/senha, por se tratar de serviços locais ao ODD, não necessitando de controles rígidos.

A viabilização do controle de acesso à serviços do sistema SDDL utilizando certificados digitais se dá através da assinatura de um texto fornecido ao usuário pelos serviços de acessos ICU e CED.

Esta assinatura a ser realizada pelo usuário deve ser efetuada utilizando a chave privada relativa ao seu certificado digital e um algorítmo de assinatura digital.

Após o texto fornecido ter sido assinado, este produto criptografado é enviado ao serviço fornecedor do acesso, o qual verifica a validade do certificado digital através de uma consulta à Lista de Certificados Revogados. Sendo válido o certificado digital o fornecedor de acesso aplica a chave pública do usuário obtida do certificado digital do mesmo, para decriptar o texto retornado pelo usuário depois de ser assinado.

Caso haja sucesso no processo de verificação de assinatura, ou seja o texto original fornecido pelo fornecedor de acesso ser recuperado, o acesso do usuário ao sistema é autorizado. Com isso garante-se a identidade do usuário que acessa o sistema,

pois somente ele tem poder de sua chave privada, parte particular fundamental do processo de assinatura digital.

Existem vários algorítmos que produzem assinatura digital, dentre os quais abordaremos o RSA e DSA mais difundidos atualmente que representam características distintas.

O RSA utiliza uma chave pública e uma chave privada para viabilizar o funcionamento do algorítmo; e a segurança do sistema está baseada na dificuldade de fatorar números grandes. No caso do RSA é gerado um resumo da mensagem, criptografado o mesmo com a chave privada do emissor e enviado o resumo assinado e a mensagem original ao destinatário.

O destinatário ao receber a mensagem e o resumo assinado descriptogra este resumo assinado utilizando a chave pública do emissor e gera um novo resumo a partir da mensagem recebida. Sendo o resumo recebido igual ao resumo gerado no receptor, garante-se a integridade da mensagem e autenticidade do emissor.

O algorítmo DSA utilizado pelo padrão de assinatura DSS também se utiliza de chave privada e função de resumo para assinar uma mensagem, tal como o RSA, mas o resultado desta assinatura a ser enviado ao receptor são somente dois números, produto final deste algorítmo de assinatura.

Estes dois números mais a mensagem original são enviados ao receptor, o qual gera o resumo da mensagem recebida e o aplica juntamente com os números recebidos e a chave pública do emissor ao algorítmo de verificação de assinatura, obtendo confirmação da integridade e autenticidade de envio da mensagem recebida..

As funções matemáticas utilizadas pelo DSA são muito diferentes do RSA, mas a segurança é semelhante utilizando-se chaves de tamanho aproximado.

Pelo motivo do uso da criptografia assimétrica no RSA e DSA podemos presumir que qualquer grande avanço na quebra do RSA também implique um avanço semelhante na quebra do DSA, e vice-versa, no que diz respeito ao uso da criptografia assimétrica.

Sendo o fator de verificação de uma assinatura digital no caso do RSA somente a função de resumo e no caso do DSA a função de resumo e números obtidos a partir da função de resumo, temos no caso do DSA um fator a mais que pode levar a um ataque ao sistema criptográfico.

Mas como ninguém foi capaz de criar ou mesmo chegar próximo à um ataque a qualquer um dos dois algorítmos, podemos concluir que não temos nenhuma vantagem expressiva de uso de um em relação ao outro, mas ocasionalmente comparações entre a velocidade e eficiência entre os dois algoritmos são publicadas dando vantagens ao uso do RSA em algumas situações.

De forma geral o uso do RSA é mais difundido do que o DSA, estando presente em grande parte das transações comerciais via Internet. Os requisitos de segurança de acesso que o SDDL exige poderiam ser atingidos qualquer um dos algorítmos, mas levando em consideração a popularidade do RSA, sua facilidade de implementação e possuir somente a função de resumo como componente envolvido na função de verificação de identidade, dando um aspecto de segurança menos crítico, sua escolha como tecnologia integrante do desenvolvimento do SDDL se faz adequada.

4.3.2 Autenticação de documentos eletrônicos

Como no caso do acesso ao sistema abordado no item acima, o sistema foi projetado originalmente para fornecer ao usuário documentos eletrônicos assinados digitalmente com base em certificados digitais do ODD, com prazo de validade limitado, ou seja sua autenticidade poderá ser comprovada localmente ao usuário num prazo determinado.

Pelo motivo de que nem todos os envolvidos em transações tenham atualmente acesso à tecnologia computacional e à Internet, documentos disponibilizados ao requerente da transação de forma eletrônica nem sempre serão interpretados.

Desta forma é disponibilizado ao usuário a opção de impressão do documento, com um frágil controle de marca d'água e a impressão ao final de um código de verificação de autenticidade a ser utilizado em acesso ao ODD para validação do documento e visualização do original digitalizado pelo ODD.

A assinatura de documentos de forma eletrônica segue os procedimentos adotados no item acima que aborda o acesso ao sistema, o qual utiliza-se a chave privada do usuário para assinar um pequeno texto fornecido pelo serviço de acesso, e utiliza-se a chave pública do mesmo para ser comprovada a veracidade da assinatura do mesmo.

Mas no caso de acesso ao sistema o texto alvo do processo de criptografia não tem associação alguma com o processo de acesso, somente serve como referência de criptografia.

Já no processo de assinatura digital de documentos eletrônicos utilizando certificados digitais, este texto a ser criptografado é o resumo da mensagem, obtido através de algorítmos de resumo tais como HMAC e SHA-1. Desta maneira o órgão disponibilizador de documentos irá:

- Gerar um resumo do documento a ser disponibilizado para o usuário.
- Assinar o resumo com base em certificado digital de validade limitada de sua propriedade utilizando um algoritmo de assinatura.
- Enviar o resumo assinado e o documento eletrônico originador deste resumo ao usuário requerente.

Na necessidade de comprovação da autenticidade deste documento o interessado de posse do documento eletrônico original e do resumo assinado pelo órgão disponibilizador:

- Obtém o certificado do órgão disponibilizador do documento.
- Verifica sua validade referenciando-se a uma Lista de Certificados Revogados.
- Aplica o algorítmo de assinatura digital a fim de verificar a autenticidade e integridade do documento disponibilizado.

No item acima foram detalhados dois algorítmos de assinatura e justificado a escolha do RSA a ser utilizado no procedimento de acesso ao sistema.

Como os procedimentos de acesso aqui utilizados tem a mesmas características utilizadas na assinatura de um documento, divergindo somente na utilização de um texto de referência no processo de acesso ao sistema e do resumo da mensagem no processo de assinatura digital do documento, conclui-se que o algorítmo RSA atende os dois casos, mesmo porque na concepção de um sistema somente devemos utilizar tecnologias diferentes para atender problemas de mesma característica quando nenhuma das tecnologias atender completamente os problemas envolvidos.

4.3.3 Comunicação com o Site da RDDE e ODDs Conveniados

A confidencialidade das informações disponibilizadas utilizando o sistema SDDL é de fundamental importância, pois não se tornaria confiável um sistema de disponibilização de informações que viesse a sofrer ataques contra a confidencialidade, integridade e autenticidade das informações disponibilizadas.

As operações de comunicação entre usuário e RDDE, usuário e ODD e ODD e RDDE viabilizadas por meio da Internet deverão fornecer segurança contra manipulação e visualização da informação durante o tráfego.

Atualmente a base da maioria das tecnologias que proporcionam segurança é a criptografia. A criptografia simétrica proporcionando cifragem de grandes blocos e fluxos de dados com alta velocidade e confiabilidade, e a criptografia assimétrica que fornece recursos de confidencialidade, autenticidade e integridade da mensagem, mescladas em protocolos criptográficos tendem a fornecer os recursos necessários à segurança da informação aliados à performance do trânsito desta informação.

O protocolo SSL *Secure Socket Layer* criado pela Netscape se utiliza de criptografia simétrica e assimétrica e foi popularizado seu uso através de Web Browsers.

A criptografia assimétrica no SSL é utilizada para estabelecimento de sessão entre cliente e servidor, operação que culmina na negociação do algorítmo e chave de encriptação simétrica que tratará o fluxo de dados que necessita de boa performance.

O SSL foi concebido para utilizar diferentes algorítmos de encriptação, autenticação e integridade dos dados, sendo a escolha do algorítmo negociada entre servidor e cliente SSL. Desta maneira temos uma negociação livre e flexível do protocolo de encriptação a ser utilizado, facilitando sua implementação.

No estabelecimento de conexão entre cliente e servidor a validação de identidade entre os envolvidos é viabilizada através de certificados digitais, a ser verificado sua validade referenciando-se à autoridade certificadora que emitiu o certificado. Desta maneira o requisito que diz respeito à validade de identidade entre os envolvidos tende a ser atingido com a utilização do protocolo SSL. Geralmente o uso de certificado digital é aplicado aos servidores que irão prover o recurso a ser utilizado, que é o caso do estabelecimento de conexão entre o cliente e RDDE ou ODD, mas a validação da

identidade dos envolvidos cliente e servidor se faz necessária na ocorrência da interação entre RDDE e ODD, a fim de evitar um possível acesso indevido às operações de interação entre RDDE e ODD.

Como a utilização do SSL desde 1994 vem sendo aprimorada nas suas versões SSLv2, SSLv3 e TSLv1, seu uso se tornou popular em diversos segmentos de comércio eletrônico, transações bancárias, etc; adquirindo uma confiabilidade não questionada atualmente.

Sua utilização em protocolos orientados à conexão e facilidade de implementação e interação com usuários comuns através de Web Browsers comuns, faz o uso do SSL no sistema SDDL uma opção de comunicação segura através da Internet que atende os requisitos necessários para fornecer:

- Confidencialidade da informação
- Autenticidade
- Integridade
- Facilidade de implementação na RDDE e órgãos disponibilizadores.
- Transparência de uso pelo usuário final.

O SSL é o protocolo de segurança mais amplamente utilizado em se tratando de comércio eletrônico, onde não se necessita de uma conexão contínua tal como ocorre com redes virtuais tal como a VPN, Virtual Private Network.

A arquitetura do SDDL originalmente não contempla conexões contínuas entre os componentes envolvidos e sim apenas interações programadas ou esporádicas com a finalidade de atualização e disponibilização de informações.

No caso da necessidade de futura integração contínua entre RDDE e algum órgão disponibilizador, a necessidade de uma VPN se torna necessária para viabilizar a comunicação entre os envolvidos por meio da Internet.

O protocolo criptográfico IPSec atualmente está sendo amplamente utilizado na maioria das VPNs instaladas, realizando a conexão virtual entre dois pontos, encriptando a informação trafegada na camada IP do protocolo TCP/IP, fornecendo confidencialidade e transparência no uso de qualquer serviço nas camadas superiores do protocolo de comunicacão TCP/IP, vindo a atender os requisitos de segurança da informação necessários para a implementação do SDDL.

4.3.4 Armazenamento de dados

O armazenamento de dados na atualidade já não representa um problema vultuoso. Os dispositivos discos rígidos fornecem grande capacidade de armazenamento e o acesso a estes dados se faz por meio de interfaces com grande capacidade de transferência.

Com o freqüente surgimento de novas tecnologias, o custo de armazenamento por byte tem reduzido ano a ano de forma significativa.

O uso de bancos de dados relacionais se faz comum na maioria das entidades, sendo implementados em várias plataformas de sistema operacional, com diferentes níveis de segurança da informação, desde os mais sofisticados até os de uso livre disponíveis à qualquer usuário na Internet.

O órgão de regulamentação da RDDE e dos ODDs conveniados terá a função de recomendar entre vários bancos de dados confiáveis disponíveis no mercado, os que atendam os requisitos de armazenamento e acesso otimizado, com a finalidade de manter um padrão de qualidade no processo de disponibilização de documentos da RDDE.

A utilização de banco de dados distribuído envolvendo a RDDE e ODDs daria um diferencial no que diz respeito à atualização quase que instantânea de informações entre os órgãos envolvidos e mudaria a concepção geral do sistema o qual envolve serviços de atualização temporal de informações RDDE – ODDs.

Mas a utilização de banco de dados distribuídos abrangendo inúmeros disponibilizadores iria requerer comunicação entre os envolvidos de boa qualidade e contínua, requisitos estes difíceis de serem atendidos pela Internet. A utilização de banco de dados distribuídos também aumentaria a exigência de requisitos quanto à qualidade do banco de dados nos ODDs que deverá fornecer características de distribuição.

Sendo que a finalidade do SDDL é se tornar popular no meio em que for implementado, entraves deste tipo que envolvem gastos financeiros com infra estrutura dispendiosa não ajudam em nada a popularização de seu uso.

Assim a interação temporal entre os envolvidos por meio da Internet para atualização de informações e a flexibilidade do uso de banco de dados de preferência do

órgão disponibilizador, desde que atenda os requisitos mínimos de segurança, ainda é a melhor forma de popularizar o uso do SDDL em diversos meios.

4.4 Especificação de funcionamento dos serviços envolvidos.

O SDDL é composto de uma série de serviços que atendem as operações de ingresso do usuário na RDDE, disponibilização de documentos e operações rotineiras dos ODDs.

A especificação de funcionamento de cada serviço individualmente e seus pontos de interação com serviços parceiros dentro do contexto relativo à operações do sistema são descritas nos itens 4.4.1, 4.4.2 e 4.4.3.

Esta especificação do SDDL envolve referencias à tabelas de armazenamento de dados cujo conteúdo e alguns campos envolvidos são abordados de forma referencial no ANEXO 1.

4.4.1 Operação Ingresso do usuário na RDDE.

A Figura 4.5 apresenta o Fluxograma detalhado das operações de Ingresso do usuário na RDDE.

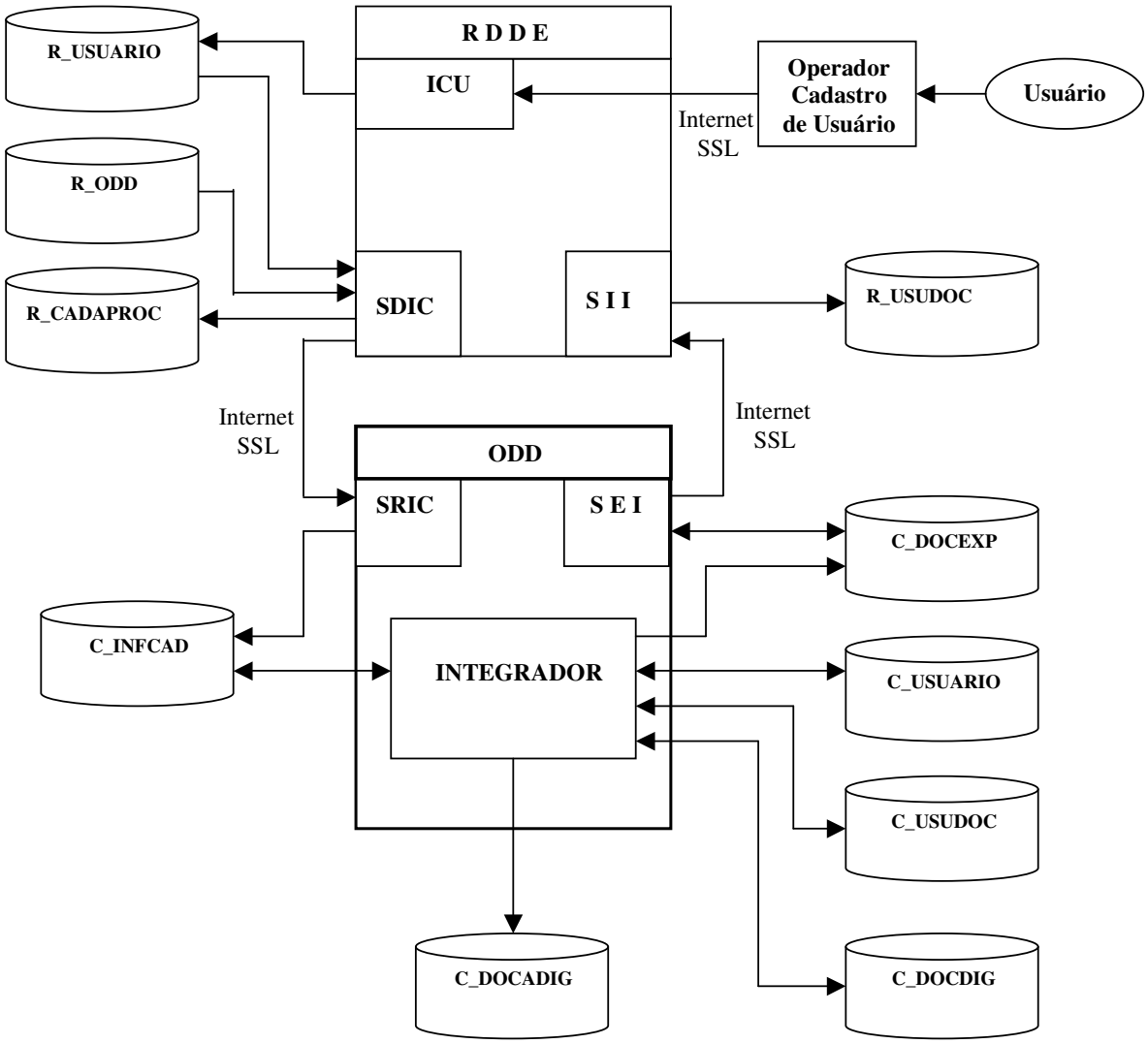

Figura 4.5: Fluxograma detalhado das operações de Ingresso do usuário na RDDE.

Serviços Envolvidos

ICU – Interface de Cadastro de Usuário

Localização: RDDE.

Função: Provê meios de inclusão e exclusão de usuários do SDDL.

Módulo Inclusão de usuário do SDDL.
Funcionamento:

- O responsável pelo cadastro de usuários na RDDE acessa o serviço ICU do SDDL localizado na RDDE via Internet utilizando sua ferramenta de navegação Web.

- É requerido sua identificação digital a fim de liberar as operações de cadastro.
- Sendo seu acesso liberado é estabelecida uma conexão segura entre seu navegador Web e o servidor da RDDE.
- Seleciona opção de inclusão de usuários do serviço ICU.
- São requeridos os dados do usuário para o qual será feito o cadastro.
- Caso o usuário tenha uma identidade digital emitida por um órgão reconhecido, seu acesso posterior ao SDDL será viabilizado com o uso de seu certificado digital.
- Caso o usuário não possua recursos de identidade digital seu acesso será viabilizado utilizando-se mecanismos tradicionais de acesso computacional, tal como usuário/senha.
- Após ser informado corretamente a identificação e dados do usuário é efetuado um registro na tabela de usuários R_USUARIO para posterior processamento e envio aos ODDs conveniados a ser realizado pelo Serviço de Disseminação de Informações Cadastrais SDIC existente no site da RDDE.

Módulo Exclusão de Usuário do SDDL.
Funcionamento:

- A exclusão de um usuário da RDDE da forma que foi concebida neste sistema, tem a sua requisição originada a pedido do usuário, tal como acorre no procedimento de inclusão de usuários.
- O responsável pelo cadastro de usuários na RDDE acessa o serviço ICU do SDDL localizado na RDDE via Internet utilizando sua ferramenta de navegação Web.
- É requerido sua identificação digital a fim de liberar as operações de cadastro.
- Sendo seu acesso liberado é estabelecida uma conexão segura entre seu navegador Web e o servidor da RDDE.
- Seleciona opção de exclusão de usuários do serviço ICU.
- Recebe opção de seleção de usuário a ser excluído da RDDE com base no código do usuário apresentado pelo próprio usuário.
- A exclusão do usuário selecionado será somente viabilizada com a validação da identidade do usuário por meio de certificado digital ou de mecanismos tradicionais tal como usuário/senha.

- Após ser selecionado e confirmado o usuário a ser excluído do SDDL , o registro deste usuário é marcado para exclusão na tabela de usuários R_USUARIO para posterior processamento pelo serviço SDIC da RDDE.

SDIC - Serviço de Disseminação de Informações Cadastrais.

Localização: RDDE.

Função: Dissemina cadastro de usuário aos ODDs conveniados.

Funcionamento:

- Executado automaticamente em freqüência pré determinada.
- Acessa a tabela de usuários R_USUARIO selecionando registros não processados.
- Acessa a tabela de ODDs conveniados R_ODD, e para cada ODD existente grava em tabela temporária R_CADAPROC os registros não processados levantados da R_USUARIO.
- Uma segunda fase do processo acessa a tabela R_CADAPROC e envia para todos os ODDs os registros não processados, removendo este registro da tabela R_CADAPROC somente após uma confirmação de recebimento enviada pelo processo SRIC do ODD.
- Caso a operação a ser realizada seja de exclusão do usuário da RDDE é efetuada uma exclusão de todos os seus dados da tabela R_USUARIO e da tabela R_USUDOC de documentos por ODD para este usuário.
- A conexão do serviço SDIC da RDDE com o serviço SRIC dos ODDs conveniados se dá via Internet através de conexão segura.

SRIC - Serviço Receptor de Informações Cadastrais

Localização: ODD.

Função: Recebe informações cadastrais do serviço SDIC da RDDE.

Funcionamento:

- Iniciado através de um pedido de conexão via Internet originado pelo processo SDIC da RDDE, quando há informações de usuários a serem atualizadas no ODD.

- As informações recebidas são armazenadas em tabela temporária cadastral C_INFCAD para posterior processamento pelo processo INTEGRADOR do ODD.
- Para cada informação cadastral recebida e gravada na tabela C_INFCAD é enviada uma confirmação de recebimento ao processo SDIC da RDDE.

INTEGRADOR – Serviço de Integração de Cadastro de Usuário

Localização: ODD.

Função: Integra dados recebidos da RDDE na base local.

Funcionamento:

- A tabela temporária C_INFCAD abastecida pelas informações cadastrais recebidas da RDDE pelo processo SRIC do ODD é então acessada.
- Para cada registro lido desta tabela procura-se uma correspondência na tabela de usuários, C_USUARIO do ODD.
- Se a correspondência levantada for total, de acordo com normas associativas pré-estabelecidas é então atualizado dados no cadastro de usuários local, tabela C_USUARIO relativo a sua relação como usuário da RDDE.
- Após ser estabelecida a relação total, informações sobre documentos existentes para este usuário no ODD cadastradas na tabela C_USUDOC são gravadas em tabela de exportação de dados C_DOCEXP, para futura integração à RDDE através do processo SEI do ODD. O processo de associação do usuário à RDDE também registra na tabela C_DOCADIG a necessidade de digitalização de documentos padrão a ser efetuado através de intervenção humana, a fim de ficarem disponíveis para sua obtenção imediata ao usuário.
- Se não houver correspondência total e somente for levantada correspondência parcial, para um ou mais usuários, o serviço INTEGRADOR grava na tabela C_INFCAD situação de correspondência parcial redirecionando o processamento de associação a ser realizado pelo processo de associação manual SAM, a sofrer interferência humana.
- Se não forem encontradas correspondência parcial ou total, qualquer operação de associação é descartada, eliminando esta informação cadastral da tabela C_INFCAD.

- Caso as informações cadastrais recebidas pela RDDE não forem de inclusão e sim de exclusão da associação do usuário à RDDE, é realizada uma atualização de dados na tabela C_USUARIO e C_DOCDIG a fim de eliminar os vínculos estabelecidos com a RDDE e eliminar documentos digitalizados agora não mais necessários por motivo da desassociação com o SDDL.

SEI - Serviço de Exportação de Informações

Localização: ODD.

Função: Dissemina informações de documentos/usuário à RDDE.

Funcionamento:

- Em execução programada os dados atualizados na tabela de exportação de dados C_DOCEXP através do processo INTEGRADOR, são por meio deste serviço enviados ao processo SII da RDDE.
- É realizada uma conexão segura através da Internet ao site da RDDE, para o envio das informações da tabela C_DOCEXP.
- Somente serão eliminados dados da tabela C_DOCEXP após a confirmação de recebimento pelo processo SII da RDDE.

SII - Serviço de Importação de Informações.

Localização: RDDE.

Função: Recebe informações de documentos/usuário dos ODDs.

Funcionamento:

- Dados enviados pelos serviços SEI dos ODDs conveniados através de uma conexão Internet segura são recebidos pelo processo SII.
- Estes dados recebidos são atualizados na base de informações de usuário/ODD/documentos, R_USUDOC da RDDE, segundo operação a ser realizada, de inclusão ou exclusão.
- Após serem atualizados os dados recebidos é enviado ao processo SEI do ODD uma confirmação de atualização efetuada com sucesso.

4.4.2 Operação Disponibilização de documentos legais ao usuário

A Figura 4.6 apresenta o Fluxograma detalhado de disponibilização de documentos legais ao usuário.

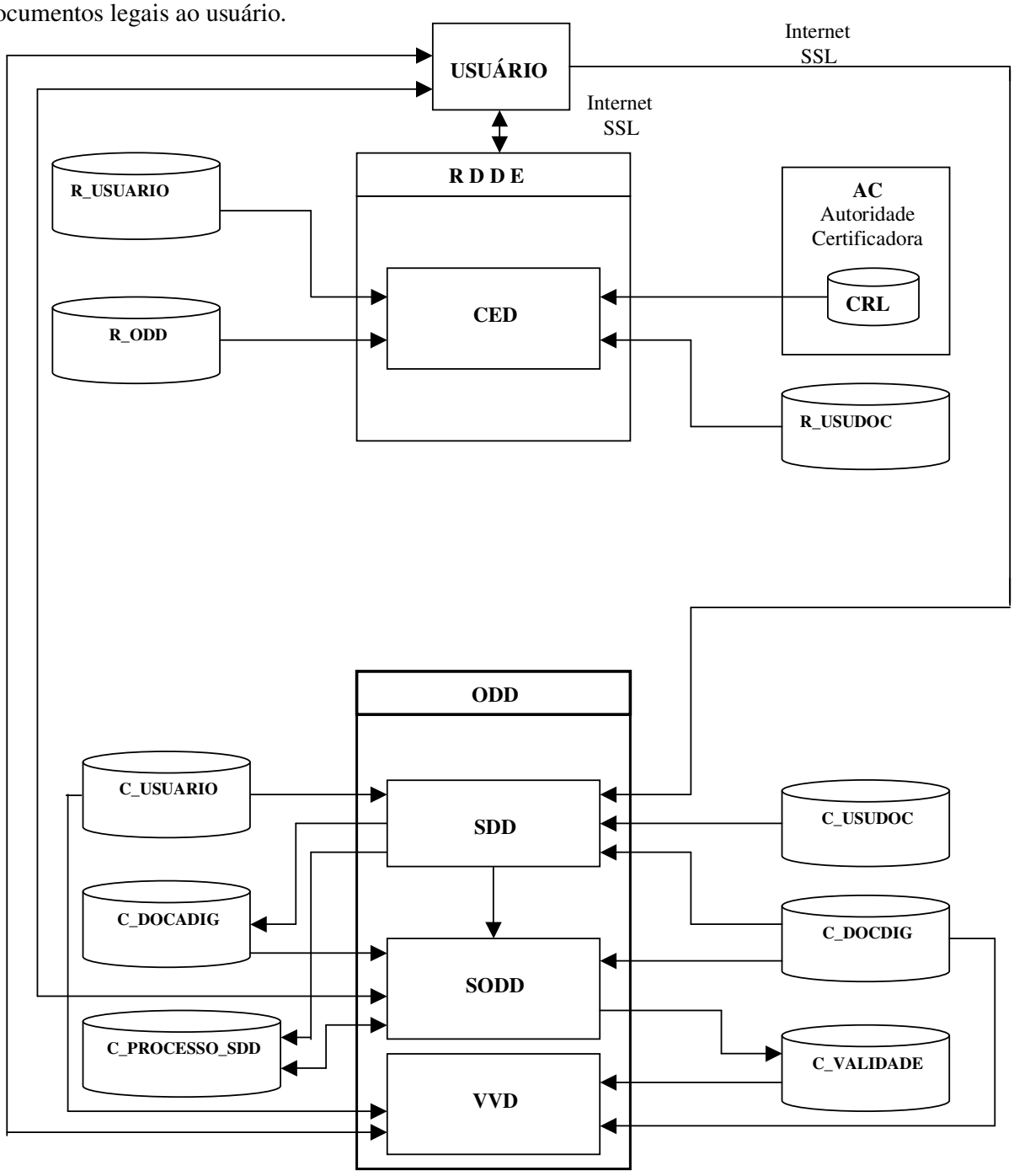

Figura 4.6: Fluxograma detalhado de disponibilização de documentos legais.

Serviços Envolvidos

CED – Consulta e Encaminhamento para Disponibilização

Localização: RDDE.

Função: Provê meios ao usuário de visualizar e solicitar disponibilização de seus documentos existentes em toda rede de ODDs conveniados.

Funcionamento:

- Usuário acessa este serviço via Internet por meio de seu navegador Web, de sua própria casa, escritório ou qualquer outro local com acesso à Internet.
- Identifica-se através de senha convencional ou utilizando seu certificado digital.
- Caso haja sucesso em sua identificação, lhe é apresentada uma interface gráfica proporcionando uma visão de todos os seus documentos em toda rede de ODDs conveniados obtido a partir da tabela R_USUDOC.
- Tendo o usuário escolhido um documento a ser disponibilizado, o serviço CED com base na tabela R_ODD e dados sobre documento a disponibilizar direciona sua conexão ao ODD detentor do documento selecionado, a fim que o serviço SDD venha a disponibilizar o documento requerido.

SDD – Serviço de Disponibilização de Documentos

Localização: ODD.

Função: Negocia parâmetros de disponibilização e encaminha obtenção do documento.

Funcionamento:

- Recebe o pedido de conexão do usuário direcionado pelo serviço CED da RDDE, informando código do usuário e código do documento a ser disponibilizado.
- Apresenta ao usuário dados que descrevem o conteúdo do documento, com base em informações obtidas através de acesso à tabela de documentos por usuário C_USUDOC.
- Acessa a tabela de documentos digitalizados C_DOCDIG, obtendo informações sobre disponibilidade imediata ou em tempo programado do documento.

- Ao usuário é requerido o prazo limite desejado para verificação da autenticidade e a escolha do modo de disponibilização do documento, seja através da impressão do documento em dispositivo local do usuário ou digitalizado e assinado digitalmente pelo ODD.
- Se o documento digitalizado estiver disponível na tabela C_DOCDIG, são então apresentadas ao usuário formas de pagamento pelo uso do recurso, baseado no tempo de validade da verificação de autenticidade. Após ter sido efetivada a transação financeira é disponibilizado ao usuário utilizando-se o serviço SODD do ODD o acesso à obtenção do documento.
- Caso o documento digitalizado não esteja disponível na tabela C_DOCDIG, serão informados ao usuário o prazo de disponibilização e um código de disponibilização a ser utilizado na obtenção do documento em prazo previsto, utilizando-se acesso direto ao serviço SODD do ODD.
- Após ter sido efetivado um pedido de disponibilização em prazo determinado, é atualizado na tabela C_DOCADIG a informação de documento/usuário a digitalizar em prazo previsto.
- Na tabela C_PROCESSO_SDD são gravadas informações sobre disponibilização do documento a serem acessadas pelo processo SODD, com base em código de disponibilização.

SODD – Serviço de Obtenção Direta de Documentos

Localização: ODD.

Função: Efetua a disponibilização do documento ao usuário.

Funcionamento:

- Recebe código de disponibilização do documento do serviço SDD ou através de acesso direto do usuário.
- Acessa a tabela C_PROCESSO_SDD com base no código de obtenção do documento obtendo informações sobre documento a disponibilizar.
- Se a opção de disponibilização selecionada for de impressão, o documento é transferido para o dispositivo de impressão selecionado pelo usuário, sendo impresso ao final um código de verificação de autenticidade, a ser informado

novamente pelo usuário ao serviço SODD, a fim de confirmar que a impressão ocorreu com sucesso e proporcionar atualização dos mecanismos de verificação de autenticidade na tabela C_VALIDADE, em prazo pré acordado.

- Se a opção escolhida for de transferência do documento digitalizado e assinado, o documento é assinado digitalmente utilizando-se dados de certificado digital do ODD com validade compatível com prazo acordado durante a transação financeira de disponibilização e disponibilizado modo de transferência do mesmo ao computador pessoal do usuário.

VAD – Verificador de Autenticidade de Documentos

Localização: ODD.

Função: Proporciona a verificação de validade da autenticidade do documento disponibilizado na forma impressa.

Funcionamento:

- Usuário interessado na verificação da autenticidade de documento disponibilizado pelo ODD acessa o serviço VAD via Internet utilizando sua ferramenta de navegação Web informando o código de verificação de autenticidade.
- Com base neste código é acessada a tabela C_VALIDADE, obtendo-se prazo de validade da verificação de autenticidade do documento e referencias de acesso à tabelas C_USUARIO e C_DOCDIG.
- Caso o prazo da validade de verificação de autenticidade não tenha expirado, é fornecido ao usuário interessado a informação de dados do usuário o qual pertence o documento e uma visão do documento digitalizado, com base nas tabelas C_USUARIO e C_DOCDIG, a fim de comparação com o documento impresso, visando garantir sua idoneidade.
- Caso o prazo de validade tenha expirado, a verificação de autenticidade do documento por meio da visão digitalizada e dados do usuário é inviabilizada.

4.4.3 Operações rotineiras dos ODDs conveniados.

A Figura 4.7 apresenta o Fluxograma detalhado de operações rotineiras dos ODDs conveniados.

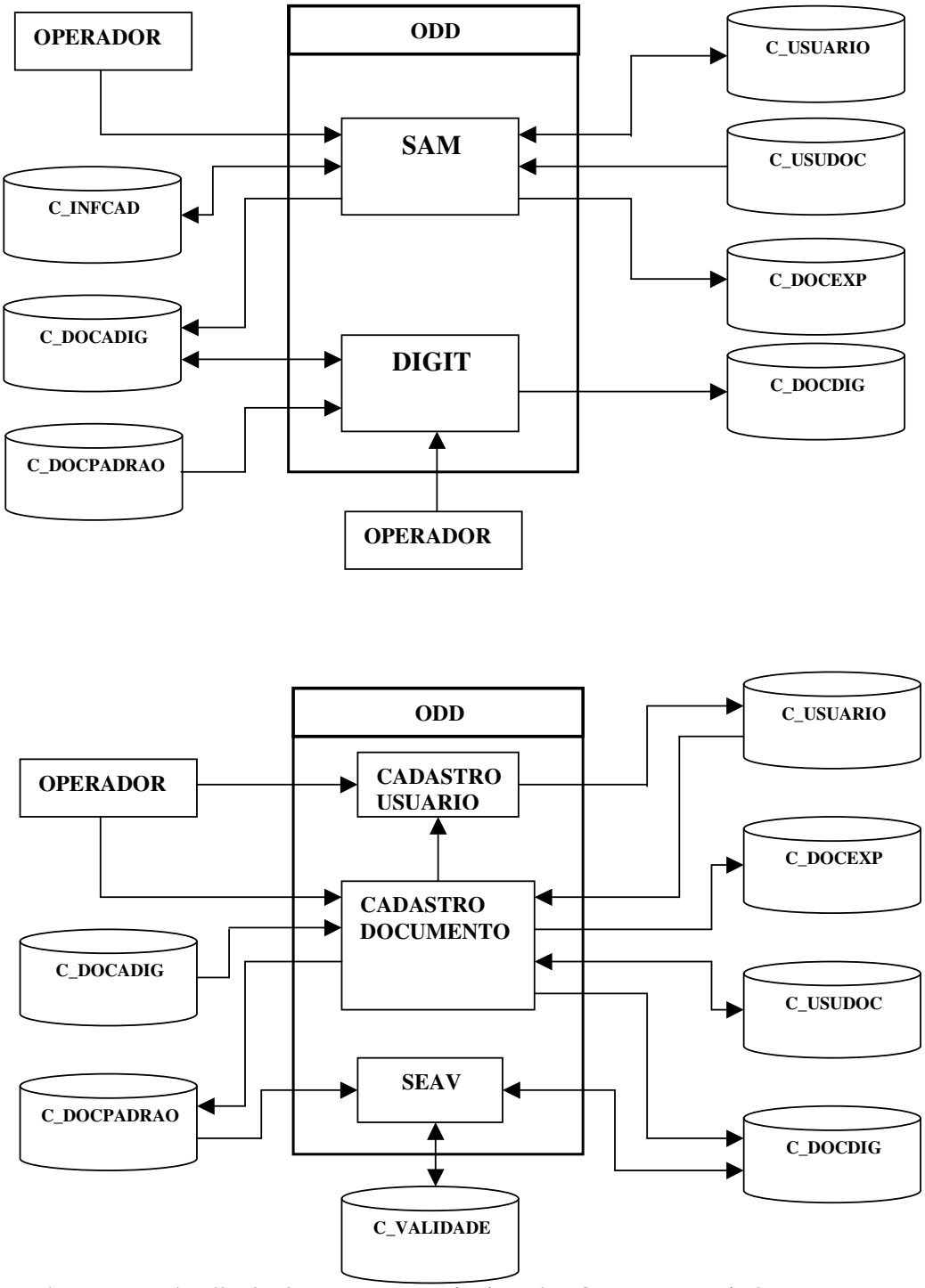

Figura 4.7: Fluxograma detalhado de operações rotineiras dos ODDs conveniados

Serviços Envolvidos

SAM – Serviço Associador Manual

Localização: ODD

Função: Tem a função de processar os pedidos de cadastros recebidos da RDDE que não tiveram correspondência total com os cadastros do ODD e sim correspondência parcial, através de intervenção humana baseando-se em regras pré estabelecidas de associação de cadastros.

Funcionamento:

- Ao operador do ODD é exigido sua identificação utilizando mecanismo tradicional de acesso, usuário/senha.
- Após ser validado o acesso do operador, a tabela C_INFCAD do ODD contendo usuários a serem integrados com correspondência parcial levantadas pelo processo INTEGRADOR é acessada.
- Para cada usuário com correspondência parcial é acessada a tabela local de usuários C_USUARIO do ODD visando selecionar um ou mais usuários do ODD que tenham correspondência parcial.
- O operador seleciona o registro que tenha comprovação total de correspondência.
- Esta seleção processa a atualização de correspondência do usuário da RDDE com usuário do ODD na tabela C_USUARIO.
- Inclui documentos padrão a serem digitalizados para este usuário na tabela C_DOCADIG e atualiza tabela de exportação de dados C_DOCEXP, com base em informações sobre documentos encontrados para este usuário na tabela C_USUDOC, a serem integrados pelo serviço SEI do ODD à RDDE, ou seja realiza grande parte dos processos do serviço INTEGRADOR, mas com interferência humana no processo de associação.

DIGIT - Serviço de Digitalização de Documentos.

Localização: ODD

Função: Receber requisição de documentos a digitalizar e integrar documentos digitalizados na tabela de documentos digitalizados C_DOCDIG.

Funcionamento:

- Ao operador do ODD é exigido sua identificação utilizando mecanismo tradicional de acesso, usuário/senha.
- É acessada a tabela de documentos a digitalizar C_DOCADIG atualizada pelos serviços INTEGRADOR, SAM e pelo cadastro de novos documentos do ODD, informando ao operador documentos a serem digitalizados para cada usuário.
- Para cada registro acessado da tabela C_DOCADIG informando código do usuário e código do documento, o operador realiza as operações de digitalização e armazenamento na tabela de documentos digitalizados, C_DOCDIG em posição relativa ao dono do documento.
- Caso o cadastro do usuário seja novo na RDDE, a digitalização de documentos para este usuário deve se basear na tabela de documentos padrão C_DOCPADRAO, a serem digitalizados para usuários da RDDE, ou seja todos os tipos documentos informados na tabela C_DOCPADRAO que o usuário tenha neste ODD deverão ser digitalizados e armazenados para este usuário.

CADASTRO USUÁRIO - Cadastro de Usuários no ODD

Localização: ODD.

Função: Efetua inclusão e/ou exclusão de usuários do ODD, atualizando associação com RDDE, caso haja.

Funcionamento:

- Ao operador do ODD é exigido sua identificação utilizando mecanismo tradicional de acesso, usuário/senha.
- Sendo seu acesso validado disponibiliza opções de Inclusão e Exclusão de usuários no ODD.
- Caso a operação seja de inclusão, o operador deve requerer os dados de cadastro ao usuário, inclusive seu código de associação à RDDE, caso possua, a fim de

estabelecer associação com RDDE para viabilizar exportação de informações de documentos existentes neste ODD à RDDE. Os dados de inclusão são atualizados na tabela C_USUARIO.

- Caso a operação seja de exclusão, após seleção de usuário a excluir é verificada a associação deste usuário à RDDE na tabela C_USUARIO. Caso seja usuário da RDDE varre a tabela C_USUDOC para este usuário e atualiza a tabela C_DOCEXP de documentos a exportar com opção *excluir* para cada documento encontrado, viabilizando assim a exclusão de documentos referenciados a ele na RDDE. Após isto elimina todas suas referências das tabelas C_USUDOC, C_DOCDIG e C_USUARIO.

CADASTRO DOCUMENTO - Cadastro de Documentos no ODD

Localização: ODD.

Função: Efetua inclusão e/ou exclusão de documentos no ODD, atualizando informações na RDDE, caso o usuário seja associado.

Funcionamento:

- Ao operador do ODD é exigido sua identificação utilizando mecanismo tradicional de acesso, usuário/senha.
- Sendo o acesso do operador validado, disponibiliza opções de Inclusão e Exclusão de documentos para usuários no ODD.
- Caso a operação seja de Inclusão são requeridos os dados do usuário e documentos a serem cadastrados para este usuário.
- Caso o usuário não esteja cadastrado, se faz obrigatório a sua inclusão no cadastro de usuários do ODD antes de prosseguir o cadastro de documentos para este usuário.
- Após ser validado a existência do usuário na tabela C_USUARIO e aceitos os dados do documento a incluir, estes dados são atualizados na tabela de documentos por usuário C_USUDOC do ODD.
- Se o usuário estiver cadastrado na tabela C_USUARIO e for usuário da RDDE, as informações sobre o novo documento para este usuário são atualizadas na tabela de dados a exportar C_DOCEXP, para posterior envio à RDDE por meio do processo SEI do ODD, e caso o tipo deste novo documento esteja incluso na tabela de

documentos padrão C_DOCPADRAO do ODD, é atualizada a tabela de documentos a digitalizar C_DOCADIG para este usuário, a se realizar em posterior operação pelo serviço DIGIT com intervenção de operador.

- Caso a operação a ser realizada seja de Exclusão de documentos, ao ser informado o código do usuário e código do documento a ser excluído este serviço elimina sua referência na base de documentos por usuário C_USUDOC e documentos digitalizados C_DOCDIG, caso exista.
- Se o usuário informado for associado à RDDE é atualizada a tabela de dados a exportar C_DOCEXP, com referência à exclusão do documento na RDDE a ser enviado pelo processo SEI do ODD.

SEAV – Serviço Eliminador de Autenticações Vencidas

Localização: ODD.

Função: Elimina da tabela C_VALIDADE registros com campo validade vencidos.

Funcionamento:

- Elimina registro da tabela C_VALIDADE que estejam com prazo de validade vencido.
- Elimina documentos digitalizados da tabela C_DOCDIG que seu tipo não estejam referenciado na tabela C_DOCPADRAO e que tiveram pedido de disponibilização com prazo de verificação de autenticidade vencida por período maior do que prazo estipulado por normas da RDDE.

4.5 Aplicação do SDDL à uma rede de cartórios

A entidade cartório é um dos ODDs que mais se ajusta ao uso do SDDL, pois é um repositório de documentos tradicionalmente conhecido o qual emite e disponibiliza documentos a diversos segmentos da sociedade, seja individual ou para entidades públicas e privadas.

Os documentos requeridos para disponibilização são geralmente exigidos com o aval de existência do cartorário, ou seja o cartorário gera uma autenticação do

documento através de sua assinatura física e um selo que identifica seu cartório. O SDDL como foi concebido provê modos de fornecer documentos autenticados de forma eletrônica aos usuários, mantendo os princípios de autenticação e armazenamento local dos documentos originais.

O uso do SDDL em entidades tipo Cartório facilitaria o funcionamento do mesmo, que poderia disponibilizar documentos autenticados sem precisar manter uma grande estrutura de atendimento pessoal. Do lado do usuário, este teria a comodidade de acesso remoto facilitado à seus documentos originais autenticados, sem dependência de deslocamento ou horários de atendimento.

Como existem diversos tipos de cartórios espalhados em todo o país, uma integração de conhecimento da informação centralizada fornece um recurso de desburocratização nacional.

O usuário interessado em fazer parte do SDDL implantado em uma rede cartorial deve comparecer a um cartório a fim de realizar seu ingresso na Rede de Disponibilização de Documentos Eletrônicos – RDDE.

Após ser cadastrado na RDDE depois de um prazo previsto, o usuário terá acesso através da Internet utilizando seu computador pessoal à informação de todos seus documentos existentes em toda rede cartorial conveniada, sem necessitar comparecer a qualquer cartório e sem depender de horário de atendimento.

Caso tenha necessidade de obter um determinando documento, o usuário deve acessar a RDDE, a qual informa os documentos disponíveis na rede cartorial e encaminha o usuário ao cartório detentor do documento requerido. Caso o documento esteja digitalizado nas bases do cartório, sua disponibilização será feita de forma imediata ao usuário diretamente ao seu computador pessoal. Caso o documento não esteja disponível, um prazo de disponibilização será informado ao usuário.

O documento de acordo com o que foi previsto pelo SDDL, será disponibilizado ao usuário digitalizado e autenticado digitalmente pelo cartório, utilizando um certificado digital com prazo de validade limitado, ou de forma a ser impresso em dispositivo do usuário com possibilidade de verificação de autenticidade, por prazo limitado viabilizada por meio de um acesso ao cartório disponibilizador do documento.

A obtenção de documentos autenticados sem restrição à deslocamento e horários de atendimento, facilita o provimento destes documentos a órgãos requerentes através

da Internet, ou seja além de termos a agilidade de obtenção de documentos dos cartórios teríamos também a agilidade de envio destes mesmos a um ou mais órgãos requerentes. Por exemplo, um processo de adoção infantil no qual documentos autenticados tem de ser enviados a várias comarcas, pode ser agilizado com o uso do SDDL

Do modo tradicional alguns documentos chegam à comarca distantes já com o prazo de validade expirado.

4.6 Comparações com outros Sistemas

O Sistema de Disponibilização de Documentos Legais de forma eletrônica SDDL, concebido neste trabalho tem a sua funcionalidade de uso em vários segmentos, sejam eles públicos e privados tais como universidades, cartórios, prefeituras, órgãos de saúde, etc.

O sistema apresenta as características já mencionadas anteriormente de:

- Segurança interna da informação nos ODDs.
- Segurança interna da informação na RDDE
- Segurança da informação trafegada entre usuário-RDDE-ODD através do uso de tecnologias que envolvem criptografia.
- Segurança de acesso ao SDDL envolvendo identidade digital.
- Descentralização da informação a ser disponibilizada.
- Visão centralizada da informação de documentos existentes de um usuário nos diversos ODDs.
- Uso da Internet como meio de comunicação entre os órgãos envolvidos.
- Disponibilização de documentos com prazo de verificação de autenticidade limitado.

Estas características fazem do SDDL um sistema que atinge os requisitos de segurança, facilidade de uso e acesso, necessários à popularização de um sistema de disponibilização de informações.

Analisando outros projetos de disponibilização de documentos, podemos nos referenciar à BDB Biblioteca digital Brasileira, que disponibiliza documentos de áreas técnicas, científicas, culturais, etc; de forma centralizada, tendo condições de receber

atualizações remotas de documentos nos vários acervos, por pesquisadores e pessoas autorizadas envolvidas na área afim.

A BDB no entanto não se preocupa com a segurança de tráfego da informação e não disponibiliza os documentos assinados digitalmente.

Outro exemplo de disponibilização de documentos eletrônicos autenticados é o projeto desenvolvido pelo cartório Azevedo Bastos, o mais antigo da Paraíba, o qual disponibiliza documentos autenticados digitalmente aos seus usuários.

O documento original ou cópia do mesmo é digitalizado e depois codificado por um software específico que o transforma a imagem em um texto legível, o qual pode ser editado e pesquisado.

Este documento então é salvo no próprio sistema do cartório servindo de base para consultas posteriores, e é gerado uma cópia em mídia digital que fica com o cliente.

O cliente pode requisitar um ou mais documentos de forma autenticada e armazenados em uma única mídia digital, servindo por tempo indeterminado para comprovar autenticidade e até o envio via Internet para órgão requerentes distantes.

Este projeto provê facilidades ao requisitante do documento autenticado, pois a partir da posse desta mídia digital contendo documentos autenticados ele não dependerá mais do cartório para obter tal serviço. Desta maneira o cartório autenticador não teria mais lucros relativos à autenticação dos mesmos.

Mesmo não necessitando comparecer à cartórios para futuras autenticações dos documentos obtidos em mídia digital, o usuário ainda depende de deslocamento ao cartório na obtenção futura de outros documentos e necessita ter conhecimento da existência de documentos nos diversos cartórios que teve relacionamento.

O SDDL atende os requisitos faltantes no que diz respeito à limitação de tempo da autenticidade de um documento dada pelo cartório e a centralização de informação e encaminhamento para disponibilização de documentos necessários.

O reconhecimento de texto legível a partir de imagem digitalizada do documento, com a finalidade de uso para pesquisas de conteúdo é muito interessante neste projeto , mas despende tempo adicional do operador de digitalização de documentos do ODD , porém poderá ser agregada esta funcionalidade no projeto do SDDL para atender casos específicos que necessitem deste recurso.

Tanto a BDB quanto o projeto do cartório Azevedo Bastos não são referências de disponibilização de documentos compatíveis com o SDDL.

O BDB abrange alguns aspectos relativos a descentralização e disponibilização centralizada e o projeto do Cartório Azevedo Bastos usa os princípios de autenticação eletrônica.

Não foram encontrados projetos compatíveis em todos os pontos com o SDDL, não havendo assim possibilidade de efetuar uma comparação relativa a melhorias e dificuldades do sistema como um todo.

4.7 Possíveis ataques e falhas do sistema.

Durante o desenvolvimento do trabalho foram levantados métodos que possibilitariam ataques ao sistema, dentre o qual relacionamos os seguintes, com a soluções adotadas para coibi-los:

- *Interceptação ou alteração de dados em acessos por meio da Internet.*

  Os pontos de acesso e transferência de dados entre ODD e usuário, entre ODD e RDDE e entre usuário e RDDE foram definidos para operarem com base em conexão segura, utilizando o protocolo SSL o qual fornece garantias de confidencialidade, autenticidade e integridade.
- *Acesso indevido aos serviços do SDDL.*

  O acesso indevido ao sistema por pessoas não autorizadas depende exclusivamente da guarda segura da chave privada, em casos de utilização de identidade digital e da senha em casos de utilização de mecanismo tradicional de acesso.
- *Entrada de dados incorretos no sistema*

  É de responsabilidade total do responsável pelo cadastro de usuários na RDDE a entrada de dados incorretos de cadastro de usuários no sistema.
- *Quebra de conexão durante processos de atualização.*

  Durante os processos de atualização de dados RDDE/ODD e ODD/RDDE caso haja queda de conexão, somente os dados que forem realmente atualizados no destino são removidos da origem, os demais dados não atualizados serão integrados na próxima operação de integração iniciada.

- *Erros de digitalização de documentos.*

  Os erros de digitalizacão de documentos são de responsabilidade do ODD, não tendo o sistema condições de criticar associação errada de documento digitalizado com documento com requisição de digitalização, pois este processo envolve procedimentos manuais do operador do ODD.

4.8 Conclusão

Este capítulo teve por finalidade apresentar os aspectos intelectuais do trabalho descrevendo a arquitetura do Sistema de Disponibilização de Documentos Legais de forma eletrônica – SDDL através de diagramas e explanações, justificando a escolha de tecnologias de segurança e armazenamento de dados aplicadas, descrevendo funcionalidades do sistema, comparando o sistema proposto com projetos semelhantes em funcionamento, detalhando o funcionamento dos vários serviços integrantes do SDDL visando esclarecer dúvidas específicas do funcionamento interno do sistema e dar apoio ao entendimento dos serviços com vistas a desenvolvimento e implantação futura.

Foram relacionados alguns tipos de ataques e falhas que o sistema pode estar sujeito e descritas soluções levantadas para coibir estas irregularidades.

As informações neste capítulo apresentadas fundamentam o desenvolvimento do trabalho, pois descrevem detalhadamente a arquitetura e funcionamento do sistema, posicionando-o dentro de um contexto de funcionalidade a ser aplicado.

5 CONSIDERAÇÕES FINAIS

O presente trabalho apresentou um sistema de disponibilização de documentos legais de forma eletrônica – SDDL, envolvendo usuários interessados nesta disponibilização, ODDs conveniados e um site centralizador de acessos que fornece uma visão global do conteúdo de documentos nos ODDs conveniados para usuários cadastrados no SDDL.

O sistema desenvolvido se utiliza de formas atuais de acesso ao sistema e autenticação de documentos eletrônicos usando certificados digitais, mas mantém também formas próximas à tradicionais para acesso e autenticação, a fim de popularizar seu uso.

Em relação ao método tradicional existente de disponibilização de documentos autenticados, o SDDL tem grande vantagem no que se refere a encurtar distâncias e tempo na obtenção de tais documentos.

O tempo de espera na obtenção de documentos ainda não digitalizados pode ser um entrave se houverem atrasos dos ODDs na execução desta tarefa, mas uma regulamentação deste procedimento estipulando prazos máximos com certeza irá favorecer o uso do SDDL.

Desde que seja viabilizada uma abrangência de grandes proporções na variedade de documentos disponibilizados de forma eletrônica e o ingresso de grande número de ODDs , o sucesso de tal projeto tende a se comprovar na prática de forma rápida.

Propostas desta natureza envolvem muitos aspectos legais e sua implementação dependeria do aval de órgãos públicos competentes.

A automação proporcionando benefício ao ser humano, na medida que encurta distâncias e reduz gastos, tende a ser aceita com facilidade por utilizadores. Mas os entraves de popularização do uso de tais recursos devem ser vencidos com a utilização de métodos de incentivo ao uso, que envolvem mais do que uma excelência tecnológica, como o bom senso na arte de encantar o usuário levando-o ao interesse espontâneo.

De nada adianta a implantação de tecnologias avançadas, sem que o principal componente, o usuário, se beneficie e gere receita que viabilize a continuidade e modernização dos recursos oferecidos.

5.1 Limitações

Tecnologias concebidas com vistas a resolver problemas reais, nem sempre conseguem atingir seu objetivo total, muitas vezes devido a entraves tecnológicos atuais ou pelo motivo da falta de popularização de avanços tecnológicos.

5.1.1 Atraso na atualização de informações entre RDDE e ODDs

No SDDL a atualização de informações do site da RDDE com ODDs e ODDs com site da RDDE não ocorre em tempo real nem em tempo hábil para que:

- Um usuário logo após sua operação de ingresso na RDDE possa visualizar informação de seus documentos existentes nos ODDs conveniados.
- Possa acessar o site da RDDE após ser gerado um documento em um determinado ODD e esta informação de novo documento gerado esteja visível imediatamente no site da RDDE.

Este atraso na atualização de informações entre RDDE e ODDs ocorre devido à limitações técnicas relativas à concepção inicial do SDDL, que teve como princípio a popularização do uso, facilidade de implantação e redução de custos da infra estrutura necessária a ser utilizada pelos ODDs. Estas limitações técnicas são devidas ao:

- Uso da Internet como meio de comunicação entre RDDE e ODDs de forma não contínua, ou seja, somente existe quando há necessidade de integração.
- Armazenamento de dados por meio do uso de banco de dados de preferência da equipe técnica do ODD, segundo diretrizes da RDDE.

Se fosse utilizada uma conexão contínua entre RDDE e ODDs de boa qualidade e os bancos de dados da RDDE e ODDs tivessem características de distribuição, as informações seriam atualizadas quase que imediatamente após cadastro do usuário ou alterações terem sido efetuadas, dando possibilidade de obtenção imediata de algum documento requerido, desde estivesse disponível na base de documentos digitalizados do ODD.

Também alguns serviços de integração tais como SDIC, SRIC, SEI e SII deixariam de existir, pois suas funções de integração esporádica perderiam o sentido de existência. Desta maneira o sistema se tornaria mais simples e ágil.

Mas a utilização de comunicação contínua de boa qualidade e o uso de banco de dados distribuído em todos os integrantes do sistema iria onerar demasiadamente os custos de implantação e manutenção do sistema. Deste modo aumentariam os custos de utilização a serem pagos pelo usuário final, custos estes que agiriam contra a popularidade de utilização do sistema.

5.1.2 Comunicação desnecessária entre RDDE e ODDs

A atualização de informações entre os ODDs e RDDE em operações de ingresso na RDDE ocorre somente quando há necessidade, ou seja, somente são transferidas informações à RDDE se o usuário realmente for associado na RDDE e se tiver documentos existentes neste ODD.

O mesmo não ocorre com a RDDE que é obrigada a interagir com ODDs que nem sempre possuem referência de documentos relativos ao usuário que está ingressando. Isto gera uma utilização desnecessária dos:

- Serviços de integração locais ao RDDE.
- Recursos de comunicação RDDE/ODD.
- Serviços de integração do ODD.

Este desperdício de recursos pode ser minimizado gerando regras de afinidade do usuário com ODDs existentes, ou seja, a integração ocorre normalmente com ODDs que possuam afinidade de localidade, interesse, etc.

Para os ODDs sem afinidade prevista os pedidos de integração podem ser agendados para momentos mais oportunos, que não venham onerar o desempenho normal do sistema.

Esta medida de contenção de integrações desnecessárias com certeza irá livrar o sistema do uso desnecessário de recursos e atenderá a maioria das integrações com sucesso, mas poderão haver casos não atendidos que venham a diminuir a confiança no processo de integração de informações da RDDE.

5.1.3 Visualização prévia do documento a ser disponibilizado

Após escolha pelo usuário do documento a ser disponibilizado através de informações sucintas fornecidas pela RDDE, o acesso do mesmo será direcionado ao ODD detentor do documento a ser disponibilizado.

O ODD fornecerá ao usuário requerente um resumo informativo do documento, que melhor o descreva, sendo que a visualização do documento original digitalizado só será permitida após realização da operação financeira que venha a cobrir as despesas da disponibilização do documento autenticado de forma eletrônica.

Esta negação de visualização prévia do documento dificulta o processo de identificação final positiva do documento correto a ser obtido, mas não podemos fornecer visualização do documento original digitalizado antes da efetivação da operação financeira, pois ao contrário esta simples visualização perante o interessado pela veracidade de existência do documento já serviria com prova necessária, sem que no entanto o ODD viesse se beneficiar financeiramente pelo uso de sua infra estrutura.

5.1.4 Autenticação com destino múltiplo.

Tradicionalmente como ocorrem em ODDs tais como cartórios, a disponibilização de documentos autenticados ocorre de maneira individual, ou seja, se o usuário necessitar comprovar autenticidade de um documento à mais de um destino interessado, ele tem que requerer um documento autenticado para cada destino, isto gera receita múltipla ao ODD.

Este tipo de controle não está implementado no SDDL, pois tornaria o processo de disponibilização complexo, tendo que ser associado cada documento autenticado à um destino interessado, o que geraria entraves no processo de disponibilização.

Sendo assim o documento disponibilizado através do uso do SDDL, serviria como meio de comprovação de autenticidade à um ou mais interessados.

Como geralmente a comprovação de autenticidade de um documento é realizada para um destino interessado, esta perda de receita não seria crítica ao funcionamento do ODD.

5.2 Trabalhos futuros

5.2.1 Implementação do sistema em plano piloto

A apresentação do sistema de disponibilização de documentos legais de forma eletrônica - SDDL concebido neste trabalho foi realizada através da definição de sua arquitetura, das tecnologias envolvidas em sua concepção e do detalhamento de funcionamento dos vários serviços envolvidos.

Com base nessas especificações, um trabalho futuro envolvendo a implementação do sistema proposto em um ambiente real poderia dar aval definitivo ao projeto concebido nesta dissertação.

A implantação de um protótipo poderia em primeiro estágio ser realizada em ambiente privado ou universidade, visando disponibilizar documentos necessários à usuários individuais ou a um grupo de pessoas com afinidade entre si.

5.2.2 Disponibilização de documentos pessoais.

A possibilidade de existência de uma área na RDDE de acesso ao usuário onde ele próprio disponibilizaria documentos menos importantes de sua propriedade, com aval de existência e validade fornecida pelo mesmo através de sua identidade digital, poderia incentivar o uso do SDDL.

5.2.3 Disponibilização agrupada.

Um trabalho futuro poderia agregar a funcionalidade do SDDL de disponibilizar documentos de forma agrupada à usuários interessados.

Sendo que em determinadas transações comerciais é requerido ao usuário o provimento de uma série de documentos autenticados, este poderia solicitar a disponibilização destes documentos autenticados através da RDDE e endereçar esta disponibilização à uma pasta virtual a existir no site da RDDE.

O parceiro comercial interessado nesta série de documentos autenticados receberia instruções sobre modo de acesso à esta pasta e obteria os documentos requeridos através de um único acesso à RDDE.

REFERÊNCIAS BIBLIOGRÁFICAS

[AJ 02] ARRUDA JR, I. **Documentos Eletrônicos, Autoridade Certificadoras e Legislação Aplicável.**
Disponível em http://www.cbeji.com.br. Acesso em: 18/04/2002.

[BRA 02] BRASIL, A. B. **Assinatura Digital Não é Assinatura Formal.**
Disponível em http://www.cbeji.com.br. Acesso em: 18/04/2002.

[BUR 02] Burnett, Steve; Paine, Stephen. **Criptografia e Segurança: O guia oficial RSA.** Rio de Janeiro: Campus, 2002. 367p.

[COS 02a] COSTA, A. A. **O Documento Eletrônico e a Assinatura Digital.**
Disponível em http://www.cbeji.com.br. Acesso em: 01/05/2002.

[COS 02b] COSTA, A. A. **Validade Jurídica de Documentos Eletrônicos. Considerações Sobre O Projeto de Lei Apresentado Pelo Governo Federal.**
Disponível em http://www.cbeji.com.br. Acesso em: 01/05/2002.

[FER 02a] FERREIRA, A. A. M. B. D. C. **E-Cartórios.**
Disponível em http://www.cbeji.com.br. Acesso em: 19/04/2002.

[FER 02b] FERREIRA, P. R. G. A **Assinatura Digital é Assinatura Formal.**
Disponível em http://www.cbeji.com.br. Acesso em: 19/04/2002.

[GAR 99] GARFINKEL, Simson; Spafford, Gene. **Comércio & Segurança na Web.**
São Paulo: Market Books Brasil, 1999. 378p.

[IBI 02] IBICT. **Biblioteca Digital Brasileira - BDB**
Disponível em http://www.ibict.br. Acesso em 04/06/ 2002.

[LAU 01] Dantas, Laurentino Augusto.
Protocolo Criptográfico para Emissão de Certidões de Nascimento na Internet
Florianópolis: UFSC 2001, Dissertação de Mestrado, Ciências da Computação.

[MAR 01] MARTINS, H. D. F. **Assinatura Eletrônica - O primeiro passo para o Desenvolvimento do Comércio Eletrônico.**
Disponível em http://www.cbeji.com.br. Acesso em: 15/04/2002.

[OLI 01] OLIVEIRA, Wilson José. **Segurança da Informação: Técnicas e soluções.**
Florianópolis: Visual Book Editora, 2001. 182p

[SCH 96] SCHNEIER, Bruce. **Applied Cryptography.** New York, NY:John Wiley &Sons,Inc., 2. ed., 1996. 675p.

[SGE 02] **O Site do Governo Eletrônico Brasília**
Disponível em http://www.governoeletronico.gov.br/ acesso em 20/03/2002

[STA 99] STALLINGS, William. **Cryptography and Network Security.**
Upper Saddle River, New Jersey:Prentice-Hall, 2. ed., 1999. 569p.

ANEXO 1 - Definição das tabelas a serem utilizadas pelo SDDL

Abaixo especifica-se as tabelas utilizadas no armazenamento de dados do SDDL em seus módulos RDDE e ODDs conveniados, com os principais campos a serem utilizados, sendo que ao longo de uma implementação do sistema poderão surgir outras necessidades aqui não contempladas.

Tabelas à existir no módulo RDDE do SDDL

Tabela: R_USUARIO

Conteúdo: Dados de cadastro do usuário na RDDE

Campo	**Descrição**
Cod_usuário	Código do usuário.
Processado	Controla atividade de processamento do cadastro
Operação	Informa operação a ser realizada no cadastro. (incluir ou excluir)
Dados do usuário	Dados cadastrais comums ao usuário (nome,cpf,etc)

Tabela: R_ODD

Conteúdo: Dados dos ODDs conveniados

Campo	**Descrição**
cod_ODD	Código do ODD
end_rede	Endereço Internet do ODD
dados do ODD	Dados cadastrais do ODD. (Nome,cgc,etc)

Tabela: R_CADAPROC

Conteúdo: Dados de cadastro de usuário a serem enviados pelo serviço SDIC da RDDE ao serviço SRIC do ODD.

Campo	**Descrição**
Cod_usuario	Código do usuário
Cod_ODD	Código do ODD
End_rede	Endereço Internet do ODD
Operação	Operação a ser realizada. (incluir ou excluir)
Dados do usuário	Dados do usuário a integrar no ODD

Tabela: R_USUDOC

Conteúdo: Dados de usuários / ODD / documentos

Campo	**Descrição**
Cod_usuário	Código do usuário
Cod_documento	Código do documento do ODD
Desc_docto	Descrição do documento
Cod_ODD	Código do ODD onde o documento foi emitido

Tabelas à existir no módulo ODD do SDDL

Tabela: C_INFCAD

Conteúdo: Dados de cadastro de usuário recebidos pelo processo SRIC do ODD, os quais foram a ele enviados pelo processo SDIC do site RDDE.

Campo	**Descrição**
Cod_usuário	Código do usuário
Operação	Operação de cadastro a ser realizada. (incluir ou excluir)
Parcial	Situação da associação do usuário com o ODD. (parcial ou nulo)
Dados do usuário	Dados do usuário a integrar no ODD

Tabela: C_DOCPADRAO

Conteúdo: Descrição de documentos a serem mantidos digitalizados para cada usuário cadastrado na RDDE.

Campo	**Descrição**
Tipo_doc	Tipo do documento
Desc_docto	Descrição do documento

Tabela: C_DOCDIG

Conteúdo: Base de documentos digitalizados disponíveis ao usuário da RDDE.

Campo	**Descrição**
Cod_usuário	Código do usuário
Cod_documento	Código do documento
Tipo_docto	Tipo do documento
Caminho	Localização de armazenamento do documento digitalizado

Tabela: C_DOCADIG

Conteúdo: Informações sobre documentos a digitalizar para serem incluídos na tabela C_DOCDIG, através de procedimentos manuais rotineiros.

Campo	**Descrição**
Cod_usuário	Código do usuário
Cod_documento	Código do documento
Prazo	Prazo para digitalização do documento pelo operador de digitalização.

Tabela: C_USUARIO

Conteúdo: Dados sobre usuários cadastrados no ODD.

Campo	**Descrição**
Cod_usuário	Código do usuário
Cod_usuário_rdde	Código do usuário na RDDE
Rdde	Controle de associação com a RDDE (sim ou nulo)
Dados do usuário	Dados gerais do usuário (nome,cpf,cgc,etc)

Tabela: C_USUDOC
Conteúdo: Dados sobre documentos por usuário disponíveis no ODD.

Campo	**Descrição**
Cod_usuário	Código do usuário
Cod_documento	Código do documento
Desc_docto	Descrição do documento
Tipo	Tipo do documento

Tabela: C_DOCEXP

Conteúdo: Informação sobre documentos a serem integradas no site da RDDE.

Campo	**Descrição**
Cod_usuário_rdde	Código do usuário na RDDE
Operação	Operação de cadastro do documento a ser realizada.(incluir ou excluir)
Cod_documento	Código do documento
Cod_ODD	Código deste ODD

Tabela: C_PROCESSO_SDD

Conteúdo: Parâmetros de processo executados pelo serviço SDD a serem utilizados pelo serviço SODD.

Campo	**Descrição**
Cod_processo	Número do processo do Sistema operacional que atendeu o serviço SDD.
Cod_usuário	Código do usuário
Cod_documento	Código do documento
Validade	Data de validade requerida pelo usuário ao documento

Tabela: C_VALIDADE

Conteúdo: Dados sobre validade de documentos disponibilizados a ser atualizada pelos serviços SODD, SEAV e acessada pelo usuário através do serviço VAD.

Campo	**Descrição**
Cod_autenticidade	Código de autenticidade do documento
Cod_usuário	Código do usuário
Tipo	Tipo do documento
Cod_documento	Código do documento
Validade	Data de validade requerida pelo usuário ao documento