

Universidade Estadual de Maringá
Centro de Tecnologia - Departamento de Informática
Especialização em Desenvolvimento de Sistemas para Web

Certificação Digital

Sandra Xavier de Macedo

Prof. Me. Ayslan Trevisan Possebom

Orientador

Maringá, 2008

Universidade Estadual de Maringá
Centro de Tecnologia - Departamento de Informática
Especialização em Desenvolvimento de Sistemas para Web

Sandra Xavier de Macedo

Trabalho submetido à Universidade Estadual de Maringá
como requisito para a obtenção do título de Especialista
em Desenvolvimento de Sistemas para Web.

Orientador: Prof. Me. Ayslan Trevisan Possebom

Maringá, 2008

Universidade Estadual de Maringá
Centro de Tecnologia - Departamento de Informática
Especialização em Desenvolvimento de Sistemas para Web

Sandra Xavier de Macedo

Certificação Digital

Maringá, ____ de dezembro de 2008

Profº Dr. Dante Alves Medeiros Filho

Ass.:_____

Profº Me. Ayslan T. Possebom (Orientador)

Ass.:_____

Profº Me. Carlos B. Sica de Toledo

Ass.:_____

AGRADECIMENTOS

Agradeço a Deus pela força que me proporcionou durante todo esse desafio.

À minha família que me incentivou a seguir em diante acreditando em mim e no meu trabalho.

Meus sinceros agradecimentos ao Professor Ayslan Trevisan Possebom, pela orientação e ajuda para a conclusão deste trabalho.

Aos Professores Dante Alves Medeiros Filho e Carlos Benedito Sica de Toledo pela presença na banca examinadora.

Aos demais amigos aqui não citados que de alguma forma me ajudaram e incentivaram.

RESUMO

Este trabalho tem com objetivo mostrar a Certificação Digital, como ela é estruturada no Brasil (ICP-Brasil), tornando seu uso de maneira segura pelo povo brasileiro e as leis envolvidas (MP 2.200-2). São apresentados os tipos de certificados pessoais tais como e-CPF e certificados de *email*, e-CNPJ, e o passo a passo para obtê-los. Também mostra como identificar um *website* seguro e como sua segurança está estruturada usando o protocolo SSL.

Ao final do trabalho, são mostrados os métodos de criptografia mais usados e seus algoritmos, incluindo suas vantagens e desvantagens. Finalmente são propostos os trabalhos futuros para os métodos de criptografia Quântica e *Wireless*.

ABSTRACT

This work has for objective to show the Digital Certification, how it is structured in Brazil (ICP-Brasil), making its use by a secure mode for Brazilian people and the laws envolved (MP 2.200-2). It presents the types of certificates for personal use such as e-CPF and email certificates, e-CNPJ, and the step by step to get them. It also shows how to identify a secure website and how this security is structured using the SSL protocol.

At the end of the work, the most used methods of cryptography and their algorithms are shown, including their advantages and disadvantages. Finally the future works are proposed for Quantum and Wireless cryptography method.

LISTA DE ILUSTRAÇÕES

Figura 2.2:	Estrutura da ICP-Brasil	18
Figura 2.2.2:	Estrutura da ICP-Brasil (AC-Raiz).....	21
Figura 2.2.5:	Autoridade Certificadora AC JUSTIÇA e suas Autoridades de Registro.....	22
Figura 3.1.1:	Encriptamento e desencriptamento utilizando Chave Secreta.....	24
Figura 3.1.1-A:	Encriptamento e desencriptamento utilizando Chaves Públicas e Privadas...25	
Figura 3.2:	Exemplo de e-CPF e e-CNPJ.....	26
Figura 3.3:	e-CPF e e-CNPJ	27
Figura 3.4:	Leitora de <i>Smart Cards</i>	27
Figura 3.5:	<i>Token</i> padrão ICP-Brasil	28
Figura 3.8:	<i>Smart Cards</i> , leitora de <i>Smart Cards</i> e <i>Token</i> padrão ICP-Brasil.....	33
Figura 4.2-A:	Interface de acesso ao formulário para obter o Certificado de <i>Email</i>	35
Figura 4.2-B:	Formulário de preenchimento dos dados do <i>email</i> a ser certificado	35
Figura 4.2-C:	Confirmação da conclusão do primeiro passo do processo	36
Figura 4.2-D:	Instalando o certificado no computador pessoal	36
Figura 4.2-E:	Conclusão da instalação do certificado pessoal de <i>email</i>	37
Figura 4.3:	Importação do certificado do usuário para o <i>Outlook Express</i>	38
Figura 4.3-A:	Gerenciador de certificados no <i>Mozilla Firefox</i>	39
Figura 4.3-B:	Salvando o <i>backup</i> do certificado no <i>Mozilla Firefox</i>	40
Figura 4.3-C:	Informando uma senha para o <i>backup</i> do certificado.....	40
Figura 4.3-D:	Lista dos certificados válidos	41
Figura 4.4:	Envio de mensagem assinada digitalmente e criptografada	42
Figura 4.4-A:	Certificado de <i>Email</i> em mensagens no <i>Microsoft Outlook 2007</i>	43
Figura 4.4-B:	Mensagem criptografada recebida	43
Figura 4.5:	Copiando o certificado do remetente	44
Figura 4.5-A:	Copiando o certificado para gerar a Chave Pública	45
Figura 5.1:	Barra de endereço seguro	47
Figura 5.2:	SSL e a pilha de protocolos TCP/IP	48
Figura 5.3:	Camadas do Protocolo SSL.....	50
Figura 5.5.3:	Formato da mensagem do protocolo <i>Handshake</i>	54

LISTA DE QUADROS

Tabela 1: Comparação entre tipos de certificados.....	29
---	----

LISTA DE SIGLAS

AC	Autoridade Certificadora
ACR	Autoridade Certificadora Raiz
AES	<i>Advanced Encryption Standard</i> (Padrão de Encriptação Avançado)
AR	Autoridade de Registro
CAC	Centro de Atendimento ao Contribuinte
CG	Comitê Gestor
CG-ICP	Comitê Gestor da Infra-estrutura de Chaves Públicas
COTEC	Comitê Técnico
CSR	<i>Certificate Signing Request</i> (Solicitação de Certificado de Assinatura)
DES	<i>Data Encryption Standard</i> (Padrão de Encriptação de Dados)
e-CNPJ	Cadastro Nacional de Pessoa Jurídica eletrônico
e-CPF	Cadastro de Pessoa Física eletrônico
ICP	Infra-estrutura de Chaves Públicas
ICP-Brasil	Infra-estrutura de Chaves Públicas do Brasil
IDEA	<i>International Data Encryption Algorithm</i> (Algoritmo Internacional de Encriptação de Dados)
ITI	Instituto Nacional de Tecnologia da Informação
MAC	<i>Message Authentication Code</i> (Código de Autenticação de Mensagens)
MP	Medida Provisória
MTI	<i>Massachussets Institute of Tecnology</i> (Instituto de Tecnologia de Massachussets)
PIN	<i>Personal Identification Number</i> (Número de Identificação Pessoal)
PKI	<i>Public Key Infrastructure</i> (Infra-estrutura de Chaves Públicas)
PRGN	<i>Pseudo Number Ramdon Generator</i> (Gerador Randômico de Pseudo Números)
PUK	<i>Personal Unblocking Key</i> (Chave Pessoal de Desbloqueio)
QKD	<i>Quantum Key Distribution</i> (Distribuição de Chave Quântica)
SISCOMEX	Sistema Integrado de Comércio Exterior
SPED	Serviço Público de Escrituração Digital
SSL	<i>Secure Sockets Layer</i>
STF	Supremo Tribunal Federal

TCP-IP	<i>Transmission Control Protocol – Internet Protocol</i> (Protocolo de Controle de Transmissão-Protocolo de Internet)
USB	<i>Universal Serial Bus</i> (Porta Serial Universal)
VPN	<i>Virtual Private Net</i> (Redes Privadas Virtuais)
WEP	<i>Wired Equivalent Privacy</i>
WPA	<i>WI-FI Protected Access</i> (Acesso Protegido Wi-Fi)

SUMÁRIO

1. INTRODUÇÃO	13
1.1 Justificativa para o Desenvolvimento do Trabalho.....	14
1.2 Objetivos do Trabalho	14
1.3 Metodologia de Desenvolvimento	15
2. CERTIFICAÇÃO DIGITAL.....	16
2.1 Lei MP 2200-02	16
2.2 ICP- Brasil (Infra-Estrutura de Chaves Públicas Brasileira)	17
2.2.1 Comitê Gestor	19
2.2.2 Comitê Técnico (COTEC) e Secretaria Executiva.....	20
2.2.3 Autoridade Certificadora Raiz	21
2.2.4 Autoridades Certificadoras	22
2.2.5 Autoridades de Registro.....	22
3. CERTIFICADO DIGITAL.....	23
3.1 Criptografia	23
3.1.1 Conceito de Chaves Secretas, Públicas, Privadas, Simétricas e Assimétricas..	24
3.2 Conceitos de e-CPF e e-CNPJ	26
3.3 <i>Smart Card</i>	27
3.4 Leitora de <i>Smart Cards</i>	27
3.5 <i>Token</i>	27
3.6 Diferenças entre <i>Smart Cards</i> e <i>Tokens</i>	28
3.7 Tipos de Certificados	28
3.7.1 Tipo de Certificado A1	30
3.7.2 Tipo de Certificado A3	30
3.8 Obtenção dos Certificados A1 ou A3.....	31
4. EMAILS E O CERTIFICADO DIGITAL	34
4.1 Conceito de Certificado de <i>Email</i>	34
4.2 Como obter um Certificado de <i>Email</i>	34
4.3 Como Instalar	37
4.4 Como Utilizar os Certificados	42
4.5 Trocando Chaves Públicas.....	44

5. PROTOCOLO SSL	47
5.1 Identificando um Site Seguro.....	47
5.2 Características do SSL	48
5.3 Camadas do SSL.....	49
5.4 Processos no SSL	50
5.4.1 Processo de Fragmentação.....	51
5.4.2 Processo de Compactação	51
5.4.3 Processo de Cifragem	51
5.5 Sessões no SSL.....	51
5.5.1 Protocolo Alert	52
5.5.2 Protocolo ChangeCipherSpec.....	53
5.5.3 Protocolo <i>Handshake</i>	54
5.6 Como Gerar um Certificado SSL.....	54
6. QUESTÕES TÉCNICAS ENVOLVIDAS NA CERTIFICAÇÃO DIGITAL.....	56
6.1. Criptografia.....	56
6.2. Tipos de Criptografias.....	57
6.2.1 Algoritmos Simétricos ou de Chave Privada.....	57
6.2.2 Algoritmos Assimétricos ou de Chave Pública.....	58
6.2.3 Função <i>Hashing</i>	59
6.2.4 Criptografia Quântica.....	60
6.2.5 Criptografia nas Redes Sem Fio.....	60
6.3 Pontos Falhos na Criptografia.....	61
CONSIDERAÇÕES FINAIS.....	62
TRABALHOS FUTUROS.....	63
REFERÊNCIAS	64

1. INTRODUÇÃO

A preocupação com a segurança na navegação na Internet hoje se tornou cada vez maior. Devido a ofertas de inúmeras facilidades dos serviços disponíveis na *WEB*, o usuário e os profissionais da área sentem a necessidade de efetivar essa segurança. Hoje temos como ferramenta a Certificação Digital que nos possibilita fazer inúmeras dessas transações de uma forma segura e ágil. O Brasil está entre os países líderes da utilização de tecnologias. Em razão disso ele se destaca também em inovações e implementações tecnológicas.

Muitos órgãos públicos brasileiros já adotaram a Certificação Digital e entre eles temos o Supremo Tribunal Federal (STF). O STF adotou a Certificação Digital em junho de 2006 com um acordo com a Caixa Econômica Federal. Desde então, os ministros do STF podem fazer os seus trâmites legais eletronicamente como se fossem pelo papel. A Receita Federal, bem como o SPED (Serviço Público de Escrituração Digital), também são usuários da Certificação Digital atualmente.

Embora seja um processo já existente há alguns anos, ele continua desconhecido por muitos usuários da web e profissionais da área. Existem estruturas, legislações e normas a serem seguidas para a efetivação da Certificação Digital, que depois de efetivadas, tornam-se, em alguns casos, transparentes ao usuário final. Para que o processo de certificação digital tenha validade, é necessário ter uma autoridade confiável que ateste e emita os certificados, uma ICP (Infra-estrutura de Chaves-Públicas). A função da ICP é a definição de técnicas, práticas e procedimentos que serão adotados pelas entidades para então ser possível um sistema de certificação digital baseado em chave pública. No Brasil, em 24 de agosto de 2001, foi definida pela Medida Provisória nº 2200-2 a Infra-estrutura de Chaves Públicas Brasileira, ou ICP-Brasil. A Autoridade Certificadora Raiz é a primeira na cadeia de certificação e executa as políticas de certificado e normas técnicas e operacionais aprovadas pelo Comitê Gestor. As Autoridades Certificadoras são organizações confiáveis (credenciadas) a emitir certificados digitais, vinculando pares de chaves criptográficas ao respectivo titular. As Autoridades de Registros (A.R.) são entidades vinculadas operacionalmente à uma determinada Autoridade Certificadora e tem a competência de identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Por meio deste estudo, pretende-se fazer um levantamento de conceitos, entidades oficiais envolvidas e os métodos utilizados para a certificação digital a fim de esclarecer o que é, como funciona o processo e como obter a Certificação Digital.

1.1 Justificativa para o Desenvolvimento do Trabalho

Tendo em vista a dificuldade para os usuários absorverem as novidades de uma maneira geral na área da informática e de identificar como proceder para assegurar a confidencialidade de seus dados na *web*, este trabalho visa esclarecer os principais pontos sobre a Certificação Digital utilizada no Brasil atualmente.

1.2 Objetivos do Trabalho

Objetivo Geral

- Será explanado o processo de certificação digital, para disseminar o seu uso e multiplicar o conhecimento de uma maneira simples, clara e precisa, abrangendo desde o mais simples usuário até os usuários com maior conhecimento na área.

Objetivos Específicos

- Abordar a estrutura existente que assegura a confiabilidade na certificação digital no Brasil, os órgãos que a compõem, sua hierarquia e qual a função de cada um;
- Quais os tipos de certificação existentes;
- Quais os tipos de certificação adotados (mais utilizados)
- Qual a aplicabilidade dos tipos existentes;
- Apresentar ao usuário, o processo para obtenção de um certificado digital para que o aplique no dia-a-dia;
- Como instalar e utilizar um certificado de *email*.
- Abordar a utilização de um site seguro, como identificar esses sites e qual o processo para assegurar os dados trafegados por ele (visão do usuário e a do gerenciador do site);

1.3 Metodologia de Desenvolvimento

O desenvolvimento do trabalho baseia-se em pesquisas realizadas por meio de sites e livros especializados no assunto referente à Certificação Digital. Sites governamentais, sites de certificadoras autorizadas e sites especializados na área de segurança da informação foram utilizados.

Inicialmente deu-se o levantamento bibliográfico e a escrita da monografia, observando os conceitos principais, leis associadas e estrutura dos órgãos envolvidos. Em seguida, foram identificadas as etapas envolvidas para o emprego da certificação digital e os órgãos certificadores.

Adicionalmente, foram realizados testes práticos envolvendo casos de certificados gratuitos em *emails*. O texto apresentado nos capítulos de 1 a 4 e parte do capítulo 5, foi propositalmente escrito em uma linguagem para usuários com ou sem conhecimentos técnicos para facilitar o entendimento dessas ferramentas pelos usuários de todos os níveis de conhecimento na área. Nos demais capítulos esse propósito não se faz possível, pois o assunto envolve a parte técnica da certificação como tipos de criptografias e o protocolo SSL.

2. CERTIFICAÇÃO DIGITAL

A certificação digital é utilizada para autenticar programas, assinaturas de mensagens, documentos eletrônicos, controle de acessos e outros.

O certificado digital é um documento eletrônico que atesta a identidade do usuário. Em outras palavras, ele é a versão digital do documento de identidade. Para que este documento eletrônico possa ser disponibilizado e utilizado pelos usuários, surgiu a necessidade de se regulamentar as atividades de certificação digital no Brasil. Foi criada então, a ICP-Brasil.

É importante conhecer toda a estrutura que envolve este processo para então se ter a confiabilidade nos resultados apresentados ao se utilizar um certificado digital.

A estrutura da ICP-Brasil foi definida pela Medida Provisória MP 2200-02. Neste capítulo será abordado o seu conteúdo, bem como o decreto 3872 de 18/07/2001 que regulamenta um dos principais órgãos da estrutura, o Comitê Gestor.

Também serão abordadas neste capítulo, as partes integrantes fundamentais para a certificação digital, incluindo os órgãos utilizados para fornecer e regulamentar tais serviços.

2.1 Lei MP 2200-02

Com o avanço da internet e suas facilidades para transações jurídicas, financeiras e comerciais, surgiu a necessidade de se criar uma lei que regulamentasse no Brasil, o acesso e a segurança nos dados transmitidos pela internet. Sendo assim, em 24 de agosto de 2001 foi criada a Lei MP (Medida Provisória) 2200-02. Esta lei tem como finalidade, definir e estruturar a Certificação Digital no Brasil. Nela foi definida a ICP-Brasil como a Infra-Estrutura de Chaves Públicas Brasileira, e também que o Brasil teria uma Certificadora Raiz, a ITI (Instituto Nacional de Tecnologia da Informação). Nesta MP (Medida Provisória), também foram elaborados os regulamentos para as atividades das entidades integrantes da ICP-Brasil. Esses regulamentos são as Resoluções do Comitê Gestor da ICP-Brasil, as Instruções Normativas e outros documentos.

2.2 ICP-Brasil (Infra-Estrutura de Chaves Públicas Brasileira)

A sigla ICP (Infra-estrutura de Chaves Públicas) vem da tradução da sigla PKI (*Public Key Infrastructure*). As tecnologias de PKI (ICP) têm como objetivo, disponibilizar meios técnicos que garantam a segurança na identificação de usuários de internet, na integridade e sigilo da informação no meio eletrônico. Em outras palavras, PKI é a solução para segurança jurídica da comunicação pela internet e de documentos eletrônicos.

A ICP-Brasil (Infra-estrutura de Chaves Públicas Brasileira) foi instituída pela MP2200-02 para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras (Art. 1º).

Ela é formada de um Comitê Gestor (CG-ICP), que é assistido por um Comitê Técnico (COTEC) e uma Secretaria Executiva. Também é formada pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz – AC Raiz, pelas Autoridades Certificadoras – AC e pelas Autoridades de Registro – AR. O modelo de Infra-estrutura adotado pela ICP-Brasil foi o de certificado com raiz única.

A Figura 2.2, (obtida no site <https://www.icpbrasil.gov.br/apresentacao/estrutura>, 2008) demonstra a estrutura da ICP-Brasil. Nela podemos observar a cadeia de autoridades que se inicia na Casa Civil da Presidência da República, Comitê Gestor e Autoridade Certificadora Raiz. Abaixo da Certificadora Raiz ficam todas as demais certificadoras que atualmente correspondem a oito organizações: Serpro, Certisign, Caixa Econômica Federal, Serasa, AC JUS, AC-PR, Receita Federal e Imprensa Oficial . A estrutura que compõe as AC e AR dessas organizações também podem ser observadas na Figura 2.2.2 na página 21 deste trabalho.

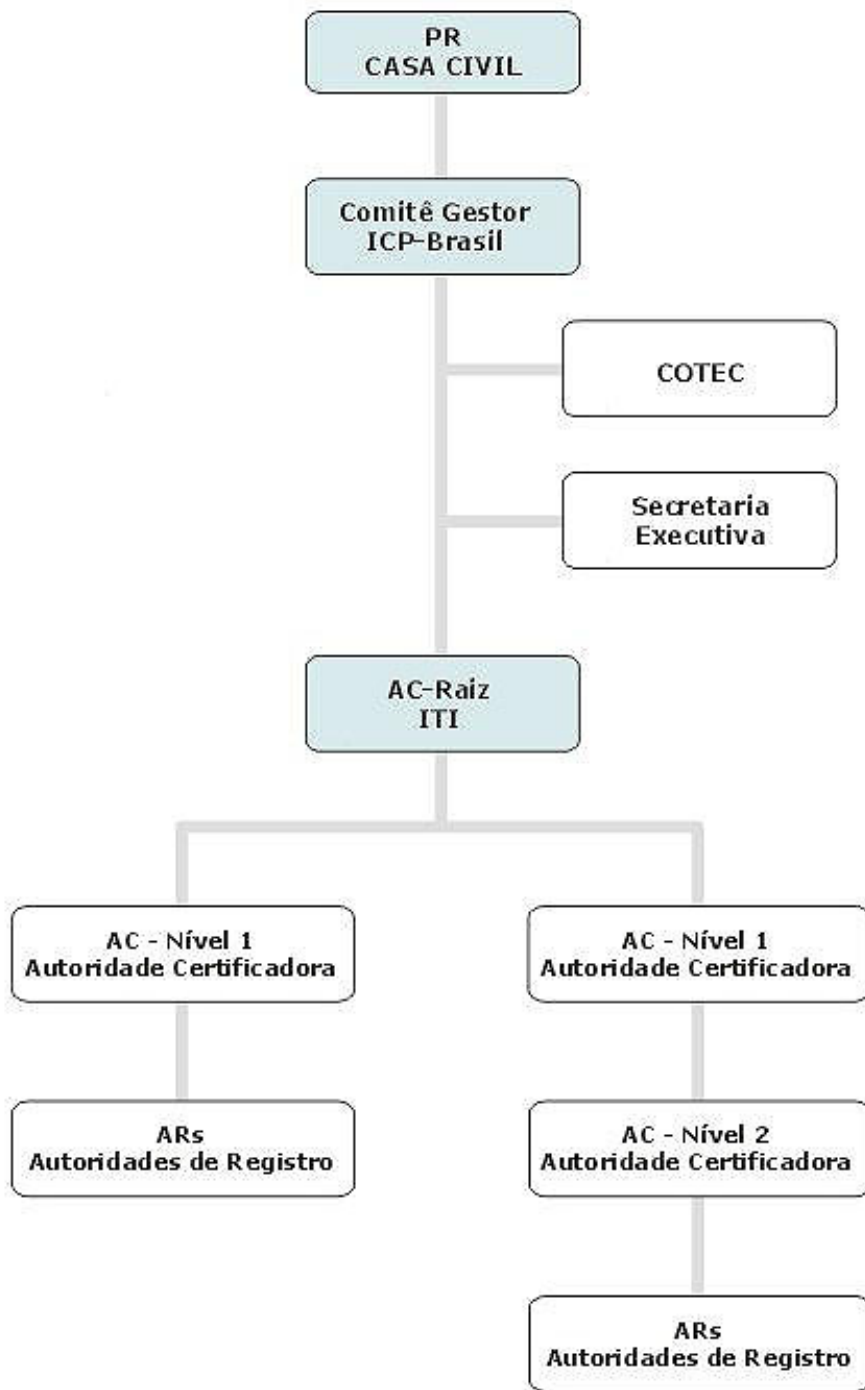


Figura 2.2: Estrutura da ICP-Brasil.

2.2.1 Comitê Gestor

O Comitê Gestor da ICP-Brasil (CG-ICP) é designado pela Presidência da República para adotar as medidas necessárias ao funcionamento da ICP-Brasil. Sua composição e competências foram estabelecidas pelos artigos 2º e 3º do decreto 3872 de 18/07/2001 respectivamente.

Segundo o Art 4º da MP 2200-2, compete ao Comitê Gestor:

- Adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;
- Estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviços de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

Várias outras competências são enumeradas no Art 4º da MP 2200, porém essas são as que mais expressam a importância do Comitê Gestor que se resume como o órgão que controla toda a estrutura e funcionamento da Certificação Digital no Brasil.

O Comitê Gestor é composto por 11 representantes, sendo cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

- Ministério da Justiça;
- Ministério da Fazenda;
- Ministério do Desenvolvimento, Indústria e Comércio Exterior;
- Ministério do Planejamento, Orçamento e Gestão;
- Ministério da Ciência e Tecnologia;
- Casa Civil da Presidência da República e
- Gabinete de Segurança Institucional da Presidência da República.

A coordenação do Comitê Gestor da ICP-Brasil é exercida pelo representante da Casa Civil da Presidência da República.

2.2.2 Comitê Técnico (COTEC) e Secretaria Executiva

O CG-ICP por sua vez é assistido pela Comissão Técnica Executiva (COTEC) que dá suporte técnico a ICP-Brasil, e de uma Secretaria Executiva (ambos especificados nos artigos 4º e 7º do decreto 3872 de 18/07/2001, respectivamente).

Segundo o portal da ICP-Brasil (2008) (<https://www.icpbrasil.gov.br/duvidas/glossary/cotec>), o Comitê Técnico (COTEC) presta suporte técnico e assistência ao Comitê Gestor da ICP-Brasil, sendo responsável por manifestar-se previamente sobre as matérias apreciadas e decididas pelo comitê Gestor.

A Secretaria-Executiva do CG ICP-Brasil (conforme Art. 6º do decreto 3872 de 18/07/2007), é chefiada por um Secretário-Executivo e integrada por assessores especiais e por pessoal técnico e administrativo.

O Secretário-Executivo é designado por livre escolha do Presidente da República (§ 1º).

É de competência da Secretaria-Executiva do CG ICP-Brasil:

- Prestar assistência direta e imediata ao Coordenador do Comitê Gestor;
- Preparar as reuniões do Comitê Gestor;
- Coordenar e acompanhar a implementação das deliberações e diretrizes fixadas pelo Comitê Gestor;
- Coordenar os trabalhos do COTEC;
- Cumprir outras atribuições que lhe forem conferidas por delegação do Comitê Gestor.

A estrutura da ICP-Brasil é composta então de uma Autoridade Certificadora Raiz, várias Autoridades Certificadoras e suas respectivas Autoridades de Registro.

Essa estrutura pode ser observada na Figura 2.2.2, retirada do site do Instituto Nacional da Tecnologia da Informação-ITI (<http://www.iti.gov.br/twiki/bin/view/Certificacao/WebHome>).

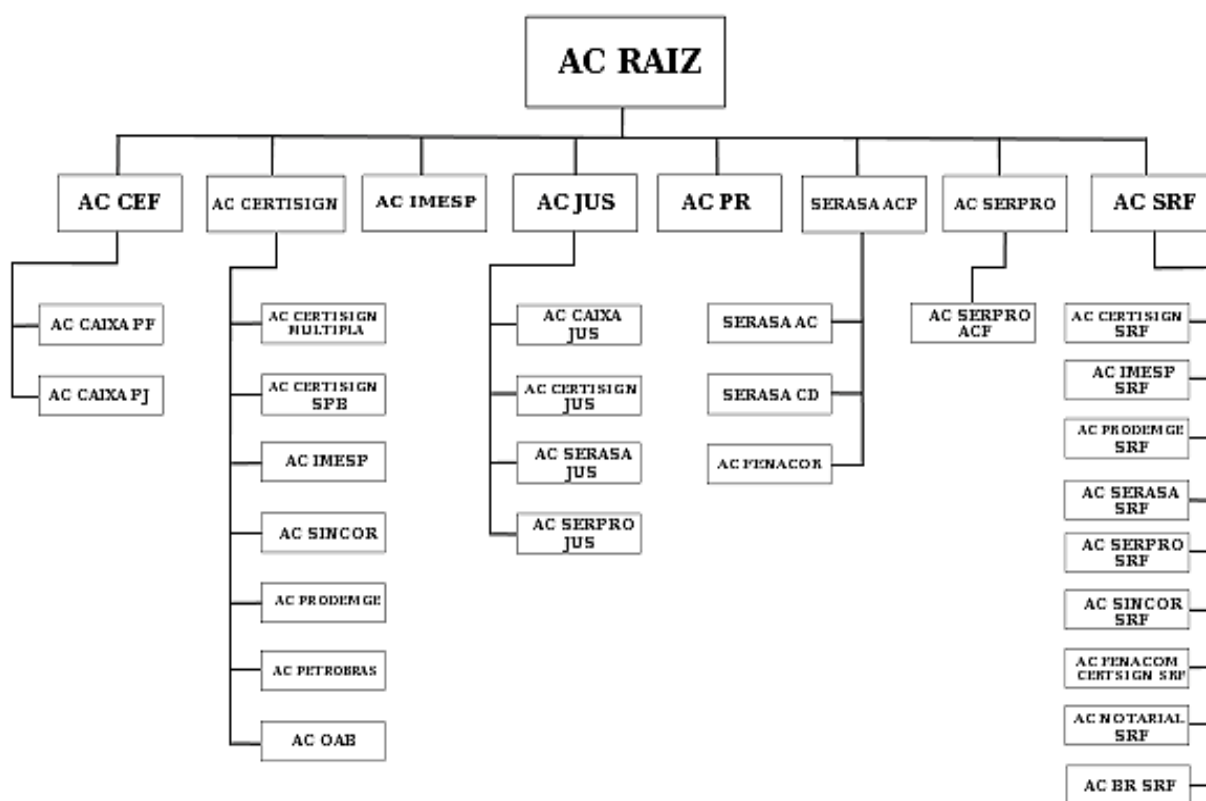


Figura 2.2.2: Estrutura da ICP-Brasil (AC-Raiz)

2.2.3 Autoridade Certificadora Raiz

A entidade que representa a Autoridade Certificadora Raiz Brasileira é a ITI - Instituto Nacional de Tecnologia da Informação. Cabe a ela credenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

A Autoridade Certificadora Raiz da ICP-Brasil, segundo Silva *et al* (2008), é a primeira autoridade da cadeia de certificação. É executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu. A AC-Raiz também está encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as Autoridades Certificadoras (AC) estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor.

2.2.4 Autoridades Certificadoras

Autoridade Certificadora é uma organização confiável que aceita aplicações certificadas de certa entidade, autentica aplicações, emite certificados e mantém atualizadas as informações sobre os estados dos certificados.

É por meio das Autoridades Certificadoras (AC) e Autoridades de Registro (AR) que a ICP-Brasil atende seus cidadãos. As AC podem ser corporativas quando atendem aos objetivos da corporação e podem ser públicas quando atendem as necessidades comuns dos cidadãos. Algumas grandes empresas optam por ter sua própria AC como é o caso da Receita Federal e Caixa Econômica. Conforme observado na Figura 2.2.5, as AC podem ser de nível 1 (AC JUS) ou nível 2 (AC CAIXA JUS), quando forem subdivididas por atividades específicas.

2.2.5 Autoridades de Registros

São entidades operacionalmente ligadas à uma determinada AC. Cabe a elas identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações. Tanto entidades privadas como órgãos públicos podem ser credenciadas como AR. A Figura 2.2.5 mostra um exemplo de Autoridade Certificadora e Autoridades de Registro.

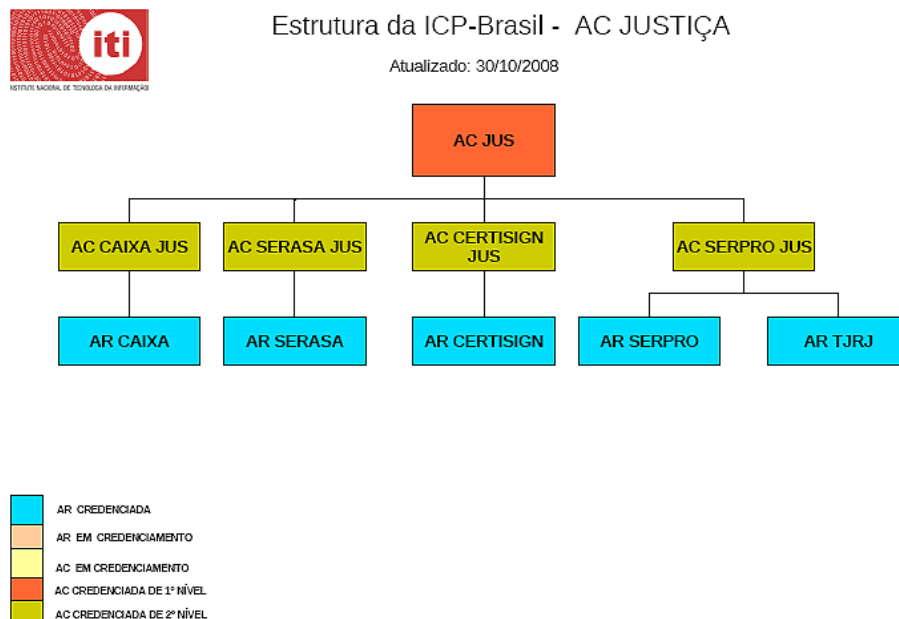


Figura 2.2.5: Estrutura da AC JUS com suas Autoridades Certificadoras e respectivas Autoridades de Registro.

3. CERTIFICADO DIGITAL

De acordo com o SERASA (2008), “o certificado digital é um documento eletrônico que possibilita comprovar a identidade de uma pessoa, uma empresa ou um site, para assegurar as transações on-line e a troca eletrônica de documentos, mensagens e dados”. Essa tecnologia permite assinar, digitalmente, qualquer tipo de documento, conferindo-lhe a mesma validade jurídica dos equivalentes em papel assinados de próprio punho.

Este capítulo apresenta os conceitos de certificados digitais e os elementos que os compõem como criptografia, chaves públicas e privadas, simétricas e assimétricas, encriptamento e desencriptamento. Também serão abordados os tipos de certificados digitais utilizados no Brasil e a função de cada um. Complementando o capítulo, será mostrado o conceito e um passo a passo da obtenção de um e-CPF ou e-CNPJ, ou seja, um certificado digital para uso de pessoas físicas/pessoas jurídicas respectivamente.

3.1 Criptografia

Para melhor compreensão do assunto a seguir, é importante esclarecer os conceitos de criptografia, chaves públicas e privadas, chaves simétricas e assimétricas.

A criptografia consiste na escrita secreta por meio de abreviaturas ou de sinais convencionados de modo a preservar a confidencialidade da informação. Segundo Silva *et al* (2008), “a criptografia é a ciência de fazer com que o custo de adquirir uma informação de maneira imprópria seja maior do que o custo obtido com a informação”.

Para a realização da criptografia, faz-se necessário a utilização de uma chave numérica. Tal chave consiste em um valor matemático gerado para ser utilizado no processo de criptografia. Pelo uso dela, serão codificadas e decodificadas as mensagens criptografadas, por meio de cálculos matemáticos.

3.1.1 Conceito de Chaves Secretas, Públicas e Privadas, Simétricas e Assimétricas

Um algoritmo criptográfico (ou processo de criptografia) usa chaves públicas e privadas para codificar o conteúdo a ser criptografado. A chave privada é conhecida apenas pelo remetente, dono da mensagem. A chave pública é enviada para os destinatários para que esses ao receberem a mensagem possam decifrar o seu conteúdo.

Quando a chave pública é igual à privada, elas são chamadas de chaves simétricas e o termo deixa de ser chave privada e pública para simplesmente chave secreta. O método utilizado é o de “Criptografia de Chave Secreta”.

As chaves simétricas funcionam muito bem numa combinação de 1 para 1, mas quando esse par de chaves (pública e privada) são as mesmas para vários destinatários, ou seja, o remetente possui a mesma combinação de chaves pública e privada para todos os seus destinatários, a segurança fica comprometida. Neste caso os destinatários teriam a mesma chave e poderiam interceptar as mensagens dos outros proprietários da mesma chave pública. Isso é solucionado com a utilização de pares de chaves assimétricas. A Figura 3.1.3 exemplifica o fluxo deste processo.

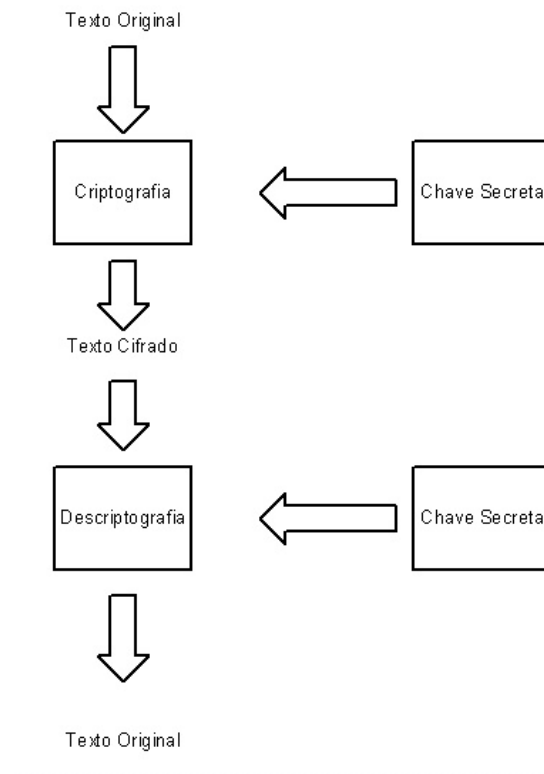


Figura 3.1.1: Encriptamento e descriptamento utilizando Chave Secreta (SILVA *et al*, 2008).

Para as chaves assimétricas, a chave privada se torna diferente para cada combinação de pares de chave (privada e pública). O algoritmo utilizado que gera esta chave é de complexidade maior, e quanto maior o tamanho da chave privada, maior será a segurança. Esse algoritmo é chamado de Algoritmo de Resumo ou simplesmente, Algoritmo Hash, conforme apresentado na seção 6.2.3.

A Figura 3.1.1-A, mostra o fluxo deste processo.

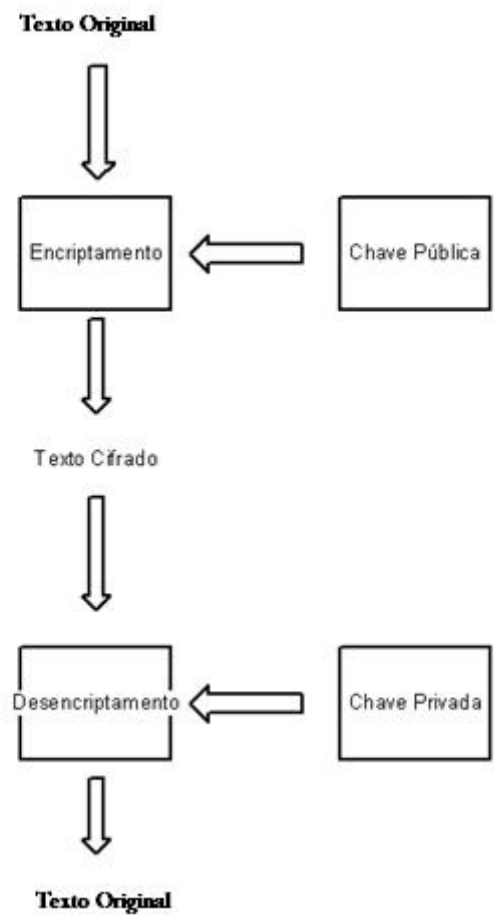


Figura 3.1.1-A: Encriptamento de desencriptamento utilizando Chaves Públicas e Privadas.

3.2 Conceitos de e-CPF e e-CNPJ

O e-CPF e o e-CNPJ são os certificados digitais que pessoas físicas e jurídicas podem usar para acessar todos os serviços online que envolvem sigilo fiscal no Brasil. Dão acesso a todos os serviços oferecidos pelo Governo Federal no meio eletrônico, como por exemplo, o SISCOMEX e o Super Simples. Com o uso destes documentos eletrônicos é possível executar estas operações com garantia de privacidade e inviolabilidade. Com o e-CPF é possível obter cópia de declarações e/ou pagamentos, realizar retificação de pagamentos, negociar parcelamentos, pesquisar situações fiscais e realizar transações relativas ao Sistema Integrado de Comércio Exterior.

Ao final de dezembro de 2005, a Receita Federal lançou o e-CAC (Centro de Atendimento ao Contribuinte) que é um canal de atendimento aos contribuintes que utilizam a internet. Para ter acesso a esses serviços oferecidos, antes limitados apenas ao atendimento pessoal nos postos da Receita, é necessário obter a certificação digital (e-CPF para pessoa física e e-CNPJ para pessoa jurídica).

O mecanismo de segurança dos certificados digitais utiliza dados criptografados durante a troca das informações e só podem ser traduzidos pelas máquinas envolvidas no processo. Isso faz com que a certificação digital se torne tão única quanto a assinatura de uma pessoa, lhe concedendo a confiabilidade para garantir transações e negócios que antes só eram efetuados por meio de documentações impressas.

O e-CPF e o e-CNPJ são geralmente certificados dos tipos A1 ou A3.

A Figura 3.2 mostra exemplos de mídia de certificado A3 (Smar Cards) para CPF e para CNPJ.



Figura 3.2: Exemplos de e-CNPJ e e-CPF.

3.3 *SmartCard*

Smart card é um cartão contendo um chip responsável pela geração e o armazenamento de certificados digitais. Neste cartão podemos gerar e armazenar chaves criptográficas que irão compor os certificados digitais. Após a geração dessas chaves, estas estarão totalmente protegidas, pois não será possível exportá-las para uma outra mídia ou retirá-las do *Smart Card*. A Figura 3.3 mostra mais um exemplo de *Smart Cards* para CPF e CNPJ.



Figura 3.3: e-CPF e e-CNPJ.

3.4 *Leitora de Smart Cards*

Para a leitura dos dados contidos nos *Smart Cards*, precisamos de um equipamento chamado de **Leitora**. A leitora é um dispositivo utilizado para conectar um cartão inteligente (*Smart Card*) a um computador. A leitora se encarregará de fazer a interface com o cartão, enquanto o computador suporta e gerencia as aplicações. Veja um Exemplo de *Leitora de Smart Card* na Figura 3.4.



Figura 3.4: Leitora de *Smart Cards*.

3.5 *Token*

É um dispositivo com capacidade de gerar e armazenar as chaves criptográficas para compor certificados digitais. Após geradas, estas chaves não poderão ser exportadas ou retiradas do *Token* (seu hardware criptográfico). Para utilizá-lo, deve-se conectá-lo em uma porta USB

(*Universal Serial Bus* – Porta Serial Universal) e instalar o driver apropriado. É possível visualizar um exemplo de *Token* na Figura 3.5.



Figura 3.5: *Token* padrão ICP.

3.6 Diferenças entre *Smart Cards* e *Tokens*

As diferenças consistem em:

- 1) Formato físico: o *smart card* é semelhante a um cartão de crédito podendo conter nome, foto e outras informações. O *Token* não tem essas características físicas podendo no máximo conter o logotipo da empresa que emitiu o certificado e tem o formato de um chaveiro.
- 2) Forma de instalação: o cartão necessita de uma leitora e drivers específicos, enquanto que o *Token* necessita apenas de um driver próprio.
- 3) Desempenho: o *Token* leva vantagem sobre o *smart card*, pois tem um desempenho em média sete vezes maior no processo criptográfico. Nos cartões esse processo se torna mais lento, pois a chave privada deve ser lida em primeiro lugar pela leitora e depois a informação é transmitida para o computador. Para o *Token* a velocidade fica limitada à porta USB.
- 4) Durabilidade: o *Token* tem durabilidade superior ao *smart card*.
- 5) Os preços praticamente se equiparam.

A escolha entre o *smart card* e o *Token* irá depender da cultura da empresa que vai utilizar. Em alguns ambientes, os cartões poderão ter uma cultura de uso mais avançada, já em outros, os *Tokens* terão maior aceitação. Ambas as mídias atendem as exigências de segurança da Certificação Digital.

3.7. Tipos de Certificados

Segundo a Resolução 41 de 18 de abril de 2006, existem 8 tipos de certificados previstos pela ICP-Brasil:

- Série A (A1, A2, A3, A4) – é composta dos certificados de assinatura digital utilizados para validar a identidade do usuário na Web, em e-mails, em redes privadas virtuais (VPN) e em documentos eletrônicos com verificação da integridade de suas informações.
- Série S (S1, S2, S3, S4) – é composta dos certificados de sigilo, que são utilizados na codificação de documentos, de bases de dados, de mensagens e de outras informações eletrônicas sigilosas.

Nos certificados do tipo A1 e S1, as chaves privadas ficam armazenadas no próprio computador do usuário. Nos tipos A2, A3, A4, S2, S3 e S4, as chaves privadas e as informações referentes ao seu certificado ficam armazenadas em um hardware criptográfico, ou seja, um cartão inteligente (*smart card*) ou cartão de memória (*Token USB* ou *pen drive*). Para acessar essas informações é necessário usar uma senha pessoal determinada no momento da compra do certificado. A Tabela 1 faz a comparação dos tipos de certificados existentes e disponíveis pela ICP-Brasil.

Chave Criptográfica				
Tipo de Certificado	Tamanho (bits)	Processo de Geração	Mídia Armazenadora	Validade Máxima (anos)
A1 e S1	1024	Software	Arquivo	1
A2 e S2	1024	Software	Smart Card ou Token sem capacidade de geração de chave	2
A3 e S3	1024	Hardware	Smart Card ou Token com capacidade de geração de chave	3
A4 e S4	2048	Hardware	Smart Card ou Token com capacidade de geração de chave	3

Tabela 1: Comparação entre tipos de certificados.

Os tipos A1 e A3 são os mais indicados para serem utilizados por pessoas físicas. O que difere de um tipo A1 para o tipo A3 é o grau de segurança que é determinado pelo modo de geração e de armazenamento das chaves criptográficas. O tipo A2 está entre os tipos A1 e A3, pois se iguala ao A1 pelo tamanho da chave e processo de geração da mesma e se iguala ao A3 pela mídia de armazenamento (*Smart Card* ou *Token*). O tipo A4 é similar ao A3, porém diferem-se no tamanho em bits da chave (2048 e 1024). A validade e o preço também variam. As mesmas comparações são válidas para a série S.

3.7.1 Tipo de Certificado A1

Tem um nível de segurança menor por ser gerado e armazenado no computador do usuário, permitindo cópias. Os dados são protegidos por uma senha de acesso. Somente com essa senha é possível acessar, mover e copiar a chave privada associada a ele. Tem validade de um ano. O certificado A1 custa em torno de 150 reais pelo período de validade.

3.7.2 Tipo de Certificado A3

Tem um nível de segurança médio a alto. É gerado e armazenado em um hardware criptográfico, que pode ser um cartão inteligente ou um *Token*. Apenas o dono da senha de acesso pode utilizar a chave privada, e as informações não podem ser copiadas ou reproduzidas. Tem validade de 3 anos e custa aproximadamente 250 reais para utilização neste período.

O Certificado Digital tipo A3 oferece mais segurança que o tipo A1 porque o par de chaves (elemento de um sistema criptográfico que protege as informações do certificado) é gerado em uma mídia apropriada, (*smart card* ou *Token*), que não permite a exportação ou qualquer tipo de reprodução ou cópia do certificado.

No par de chaves, uma é chamada de chave pública e a outra de chave privada. A chave pública é enviada para a AC junto à solicitação de emissão do certificado e servirá para identificar o seu titular nesse e em outros processos durante a validade do certificado. A chave privada ficará armazenada no cartão inteligente para autenticar os processos nos quais o certificado for utilizado.

Para que um certificado seja emitido, é necessário solicitá-lo pela internet, cadastrando uma senha de identificação alfanumérica. Depois, é preciso validá-lo presencialmente em um ponto de atendimento credenciado, mediante agendamento prévio. Lá, um agente de validação receberá a documentação necessária. Finalmente, será solicitado que as senhas padrão do certificado sejam alteradas. Essas senhas devem ser uma *password* e/ou *PIN* (*Personal Identification Number* – Número de Identificação Pessoal) e *PUK* (*Personal Unblocking Key* – Chave Pessoal de Desbloqueio) de conhecimento exclusivo do titular. No caso do *Token*, é utilizada somente a senha *PIN*.

Com o Certificado Digital tipo A3, o usuário transporta a sua chave privada de maneira segura, realizando transações eletrônicas onde desejar, com garantia de segurança e integridade das informações.

3.8 Obtenção dos certificados A1 ou A3

Com base nos textos apresentados por Gisele Ribeiro, os seguintes passos descrevem as ações que o usuário deve executar para a obtenção de um certificado digital de tipo A1 ou A3:

1) Fazer a solicitação:

- a) Entrar no site de uma das autoridades certificadoras credenciadas pela ICP-Brasil (podemos citar como exemplo a Receita Federal, Caixa Econômica, *CertiSign*, Serpro, Serasa).
- b) Preencher uma solicitação.
- c) Neste ponto é possível optar pelo tipo (A1 ou A3) e a forma de pagamento do certificado, que pode custar em torno de R\$ 150,00 para o tipo A1 e R\$ 250,00 para o tipo A3. O preço vai depender do tipo e da autoridade certificadora escolhida. Caso o certificado escolhido seja o A3, antes de fazer a solicitação, será necessário adquirir um dispositivo de armazenamento (*Token* ou cartão inteligente) e instalar o driver desse dispositivo no computador.

2) Ir até uma Autoridade de Registro (AR).

- a) Deve-se marcar um horário de atendimento na Autoridade de Registro da Autoridade Certificadora escolhida para o atendimento presencial;
- b) Lá devem ser apresentados os documentos solicitados:

c) Os documentos exigidos para o e-CPF devem ser originais ou cópias autenticadas e são:

- cédula de identidade ou passaporte (se estrangeiro);
- CPF;
- comprovante de residência (emitido há, no máximo, três meses);
- foto 3x4 recente;
- comprovante de depósito de pagamento do certificado e
- termo de titularidade devidamente preenchido.

O número de identificação social, título de eleitor e o cadastro específico do INSS são opcionais.

d) Já para o e-CNPJ, são necessários:

- o registro comercial (em caso de empresa individual);
- o ato constitutivo;
- estatuto ou contrato social em vigor;
- o CNPJ e
- os documentos da pessoa física responsável pela certificação (cédula de identidade, CPF, comprovante de residência e uma foto 3x4).

O cadastro específico do INSS, termo de titularidade e de responsabilidade devidamente preenchido e o comprovante de depósito de pagamento do certificado também são opcionais para este caso.

Toda essa documentação é conferida, e caso esteja correta, os representantes da empresa devem assinar um termo de titularidade, na presença de um funcionário responsável por sua identificação física.

3) Obtenção do Certificado Digital para iniciar o uso:

a) Após isso, é possível baixar o certificado pela internet (tipo A1) ou então pegar o *Smart card*, ou o *Token*, na própria autoridade de registro (tipo A3). A Figura 3.8 mostra exemplos de *Smart Cards*, Leitora de *Smart Cards* e um *Token*, utilizados para certificados do tipo A3.



Figura 3.8: *Smart Cards* (e-CPF e e-CNPJ), leitora de *Smart Cards* e *Token* padrão ICP.

4. EMAILS E O CERTIFICADO DIGITAL

A necessidade de segurança em *emails* surge quando ocorre a violação destes ou mesmo quando não se tem a certeza de que estes não tiveram o conteúdo violado. São muitas informações sigilosas que trafegam na web por meio de *emails*. Para o usuário que tem essa necessidade de sigilo, é possível empregar o uso do certificado de *email*. Neste capítulo será apresentado o Certificado de *Email* mostrando passo a passo como obter um gratuitamente e como utilizá-lo em mensagens assinadas digitalmente e/ou criptografadas.

4.1 Conceito de Certificado de *Email*.

O certificado de *email* é um registro das informações do usuário em conjunto com endereço do seu *email*. Essas informações ficam registradas em uma Autoridade Certificadora credenciada, sendo que esta pode ser estrangeira. Ao fazer o “cadastro” destas informações necessárias na Autoridade Certificadora escolhida, é gerado um arquivo com o certificado deste *email* cadastrado. Apenas um certificado para cada endereço de *email* pode ser gerado em cada certificadora. O certificado do *email* é então enviado para o endereço de *email* correspondente podendo ser instalado no programa gerenciador de *emails* do usuário (ex. *Outlook* da *Microsoft*, *Thunderbird* da *Mozilla*).

4.2 Como obter um Certificado de *Email*

Hoje podemos obter um certificado de e-mail de forma gratuita. Atualmente não encontramos no Brasil, uma certificadora que forneça um certificado gratuito de email por um intervalo de tempo acima de 30 dias. É possível, porém, utilizarmos uma certificadora estrangeira para estes serviços. Podemos citar como exemplo o site da certificadora www.comodo.com. Ela disponibiliza este serviço gratuitamente bastando acessar o site onde se encontra a interface conforme a Figura 4.2-A a seguir. É importante lembrar que este certificado será instalado no computador de onde ele foi requisitado. Para transportá-lo para outra máquina, é necessário fazer um backup do arquivo e executar o processo de instalação novamente. A seguir será demonstrado o processo passo a passo para a obtenção do certificado de *email* na Certificadora Comodo, no site www.comodo.com.

Passo 1: Informar o endereço www.comodo.com na barra de endereços do seu browser;

Passo 2: Ao selecionar a opção “*FREE Email Security Certificate*”, será apresentada a tela conforme a Figura 4.2-A.

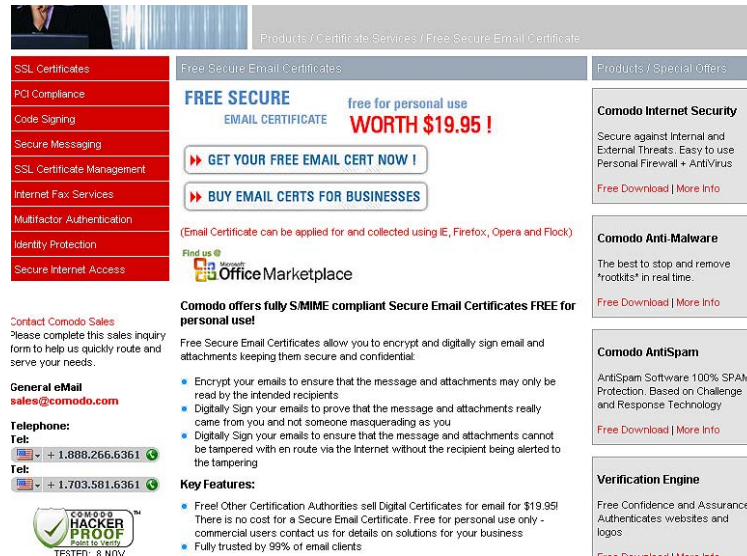


Figura 4.2-A: Interface de acesso ao formulário para obter o certificado de *email*.

Passo 3: Nesta tela, selecione a opção “*GET YOUR FREE EMAIL CERT NOW!*”. Ao selecionar esta opção, será apresentado o formulário para preenchimento dos dados sobre o *email* que utilizará/receberá o certificado (Figura 4.2-B)

C·O·M·O·D·O

Application for Secure Email Certificate

Your Certificate Details
These details will be visible to people who use your certificate. They are required:

First Name: Michel
Last Name: Ferid
Email Address: michelferyd@gmail.com
Country: Brazil

Private Key Options
Key Size (bits): Nível médio

Revocation Password
If you believe the security of your certificate has been compromised, it may be revoked. A revocation password is required to ensure that only you may revoke your certificate:
Revocation Password:
Re-enter Revocation Password:

Comodo Newsletter Opt in?

Subscriber Agreement
Please read this Subscriber Agreement before applying for, accepting, or using a digital certificate. If you do not agree to the terms of this Subscriber Agreement, do not apply for, accept, or use the digital certificate.
entering into this agreement which relates to the provisions and subject matter of this

Secure Email Certificates
Step 1: Provide details for your certificate
Step 2: Collect and install your certificate

Figura 4.2-B: Formulário para preenchimento dos dados do *email* a ser certificado.

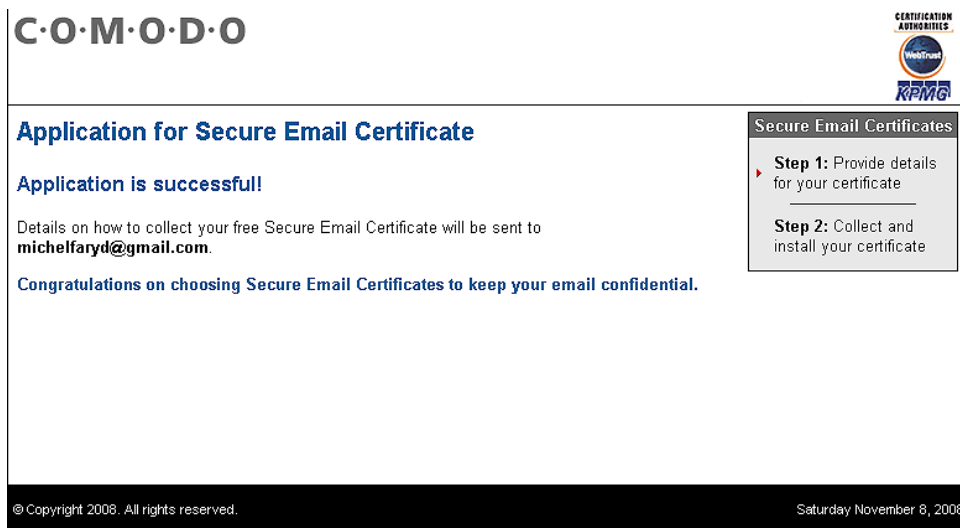


Figura 4.2-C: Confirmação da conclusão do primeiro passo no processo.

Após este passo, será enviado o *email* com o *link* que será acessado ao clicar no botão vermelho conforme pode ser observado na Figura 4.2-D. Caso ocorra algum problema de acesso, podemos acessar via browser utilizando o *link* e senhas de ativação, mencionados logo abaixo deste botão.

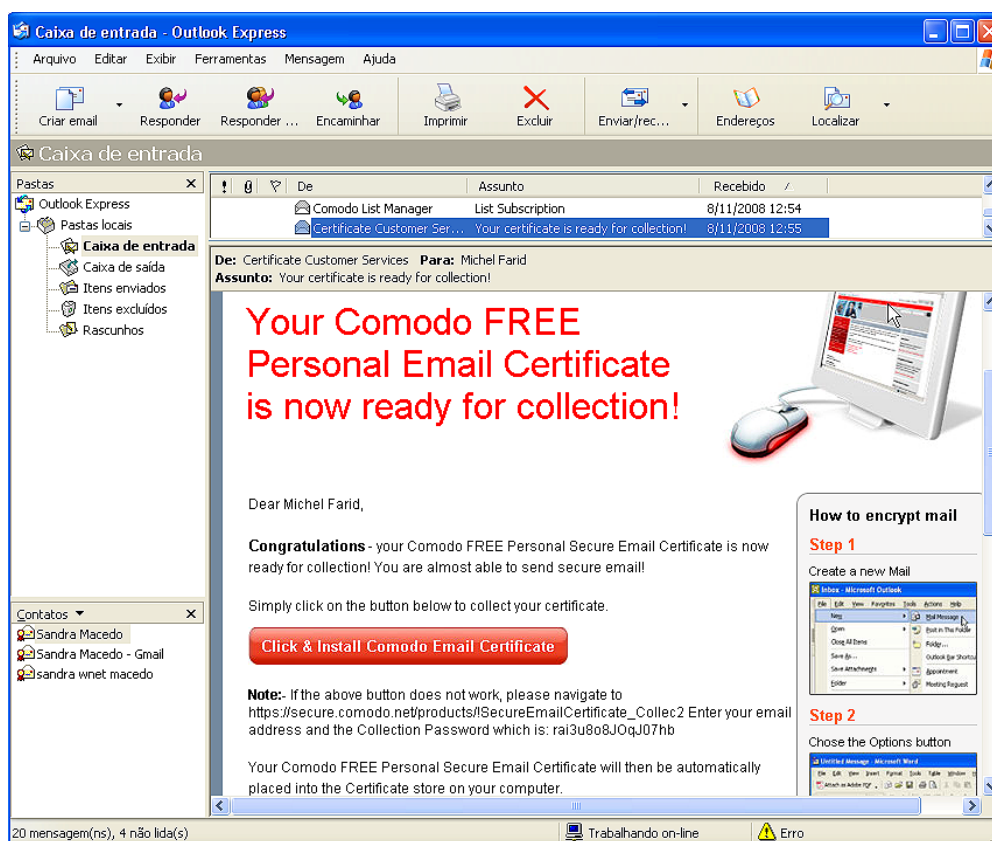


Figura 4.2-D: Instalando o Certificado no computador pessoal.

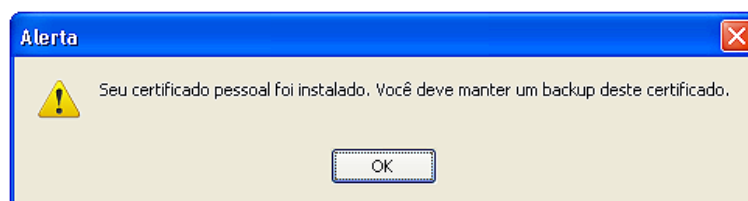
Após este processo, a certificadora emite a mensagem conforme a Figura 4.2-E a seguir:

C·O·M·O·D·O



Collection of Secure Email Certificate

Attempting to collect and install your Free Certificate...



Secure Email Certificates

- ✓ **Step 1:** Provide details for your certificate
- ▶ **Step 2:** Collect and install your certificate

© Copyright 2008. All rights reserved.

Saturday November 8, 2008

Figura 4.2-E: Conclusão da instalação do certificado pessoal de *email*.

Após esta etapa, o certificado já está presente no computador do requisitante, sendo necessário que se faça a importação para o gerenciador de *email* para que possam ser efetivamente utilizados.

4.3. Como instalar

Os certificados de *email* devem ser instalados nos gerenciadores de *email*. Aqui neste trabalho serão demonstrados exemplos utilizando o gerenciador de *email* da *Microsoft* nas versões *Outlook Express 6.0* e *Outlook 2007*.

Conforme visto no item anterior, logo ao obter um certificado, é especificado o endereço de *email* para o qual o certificado terá validade. Será enviada uma mensagem com o *link* para a ativação deste certificado, bem como a sua instalação. Este processo de instalação é praticamente transparente para o usuário que está instalando o certificado, porém é necessário concluir a instalação executando os passos descritos na página 38. Esses passos podem ser observados na Figura 4.3, utilizando o *Outlook Express 6.0*. O processo é semelhante para o *Microsoft Outlook 2007*.

Passo 1: Utilizando o *Outlook Express* 6.0, acesse o menu Ferramentas, Contas, selecione a conta que receberá o certificado e clique em propriedades;

Passo 2: Selecione a aba “Segurança”;

Passo 3: Clique no botão “Selecionar” do Certificado de Autenticação;

Passo 4: Selecione o certificado que deseja usar, conforme solicitado na interface e clique em OK.

Passo 5: Clique no botão “Aplicar”, Ok e Fechar.

A Figura 4.3 exibe o certificado do usuário Sandra Macedo para ser importado para o *Outlook Express*.

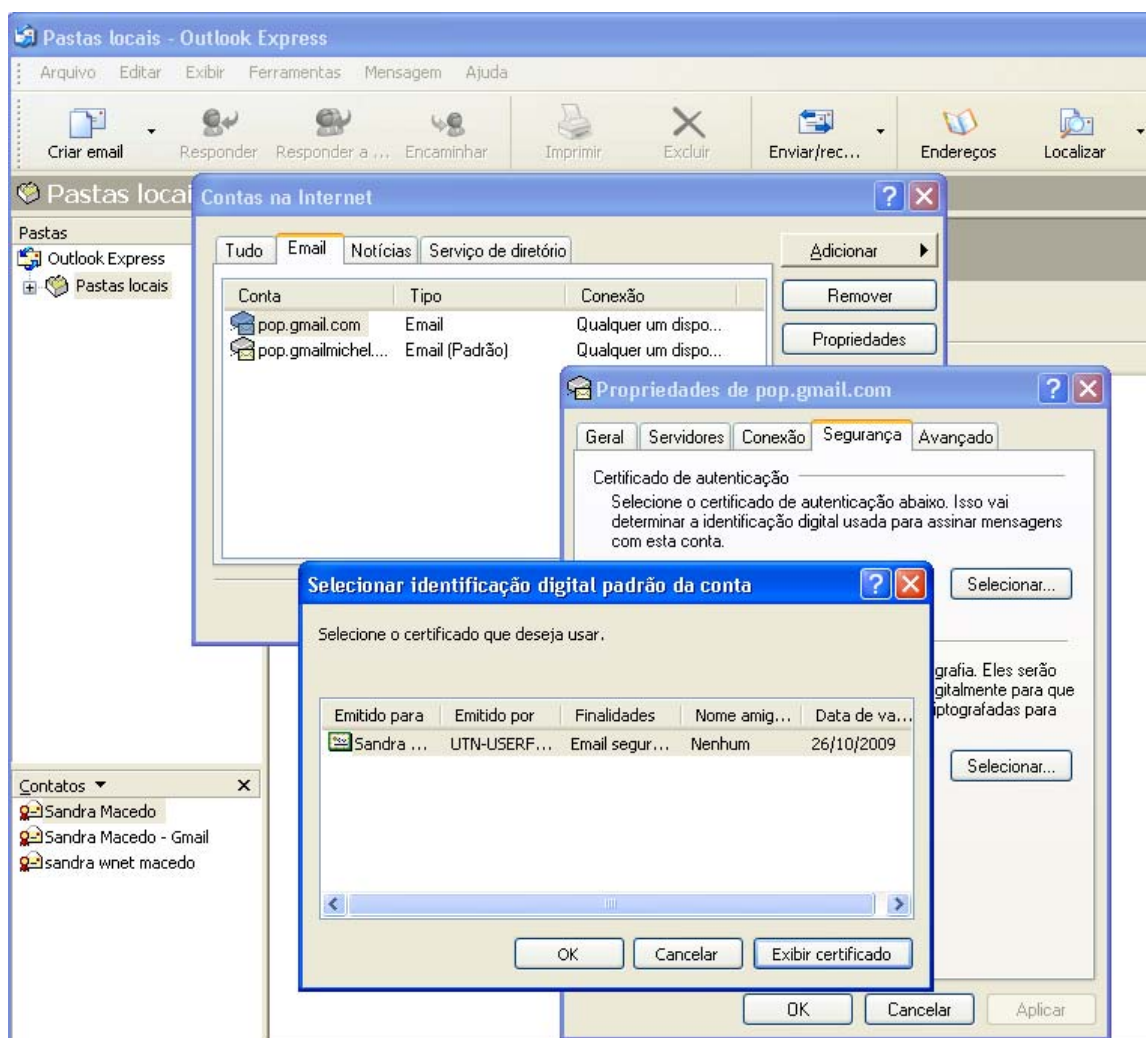


Figura 4.3: Importação do certificado.

Caso o certificado não seja encontrado na interface descrita no passo 4 deste processo, pode ter ocorrido alguma falha ao receber o certificado automaticamente no Passo 3 do processo anterior (Como obter um certificado de *email*). Isso pode ocorrer devido à incompatibilidade de browsers, ou seja, utilizar browsers e gerenciadores de *email* de softwares diferentes. Por

exemplo: utilizar o browser *Mozilla Firefox* e o gerenciador de *email Outlook Express*. Para solucionar esta questão basta exportar o certificado pelo browser no qual ele foi obtido para um arquivo salvo no disco, e em seguida importá-lo pelo browser compatível com o gerenciador de *email*. O exemplo a seguir utilizará um certificado solicitado pelo *Mozilla Firefox* para ser utilizado no *Outlook Express 6.0*. Acompanhe os seguintes passos:

Passo 1: No *Mozilla Firefox*, acesse a opção “Ferramentas /Opções /Avançado /Certificados /Seus Certificados”, (Figura 4.3-A). Nesta interface estarão os certificados obtidos.

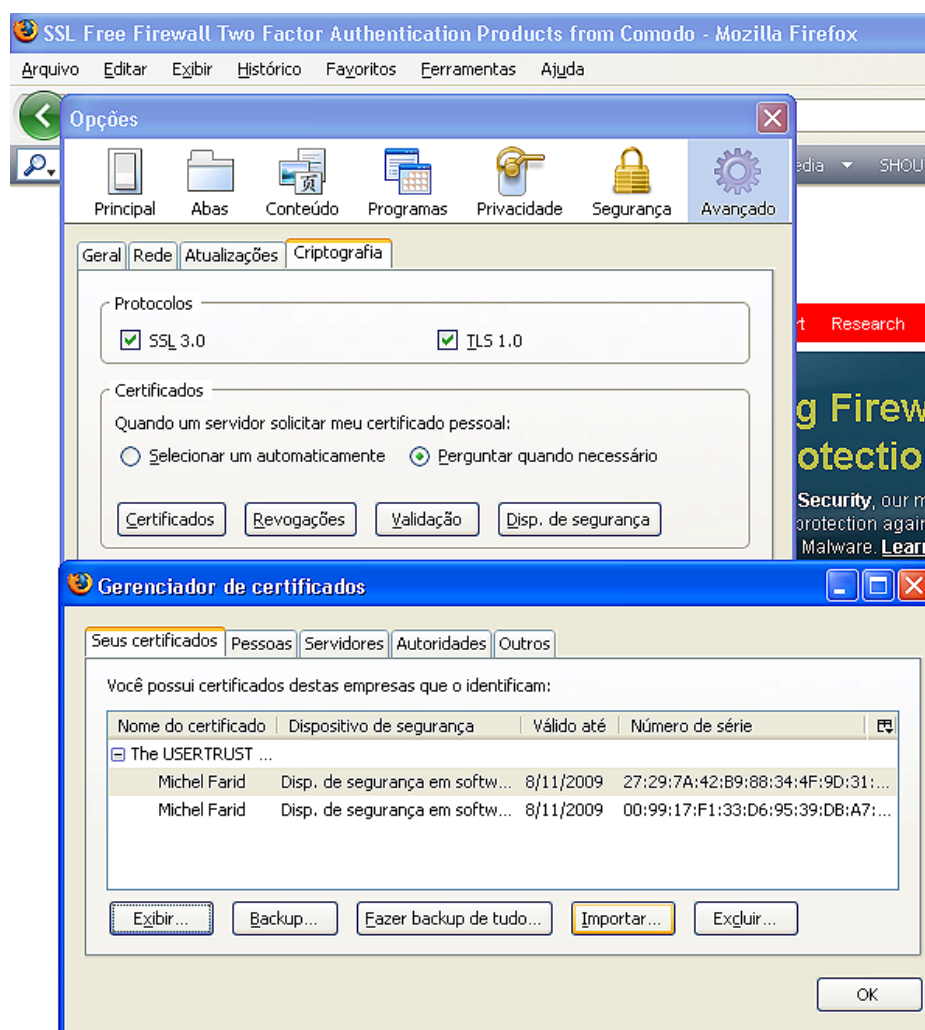


Figura 4.3-A: Gerenciador de Certificados no *Mozilla Firefox*.

No Internet Explorer, acesse em Ferramentas/Opções de Internet/Conteúdo/Certificados.

Passo 2: Selecione o certificado na lista apresentada e faça um backup do certificado clicando no botão Backup.

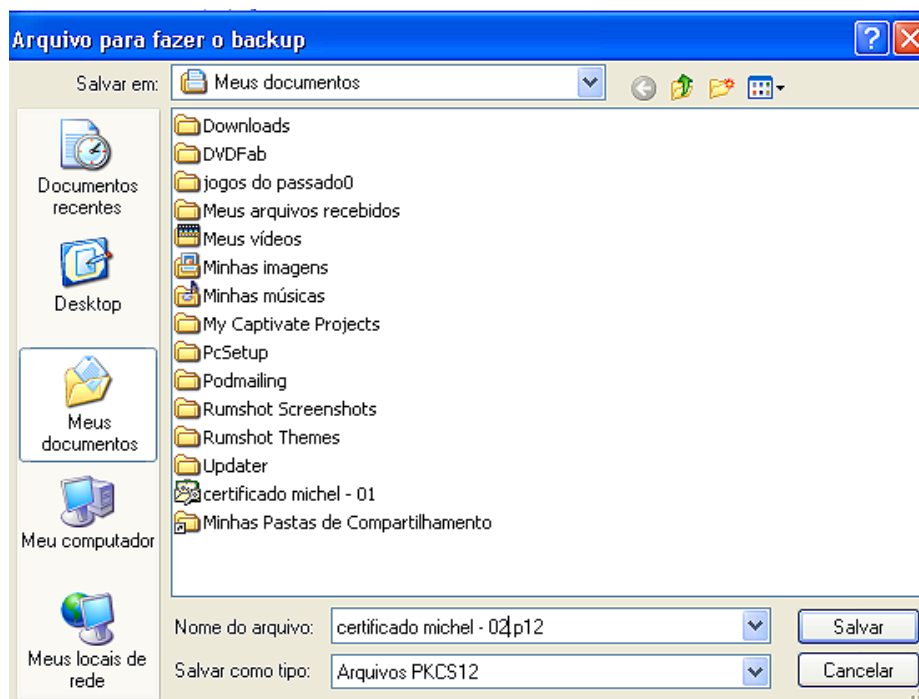


Figura 4.3-B: Salvando o backup do certificado no *Mozilla Firefox*

Passo 3: Deve ser especificada uma senha para o backup do certificado. Informe uma senha e clique em OK.



Figura 4.3-C: Informando uma senha para o backup do certificado

Após este procedimento, deve ser importado o certificado no browser compatível com o gerenciador de *email*. Neste exemplo utilizamos o *Internet Explorer* acessando Ferramentas /Opções de Internet /Conteúdo/Certificados. Nesta interface, o certificado deve ser importado. Antes de ser importado, ele não aparecerá na lista de certificados. Neste caso, clique em

“Importar” e localize o arquivo exportado pelo *Mozilla Firefox* no procedimento anterior. Após isso, o certificado estará nesta lista apresentada na figura a seguir. A figura 4.3-D exibe a lista de certificados válidos para utilização nos gerenciadores de *email* compatíveis com o Internet Explorer.

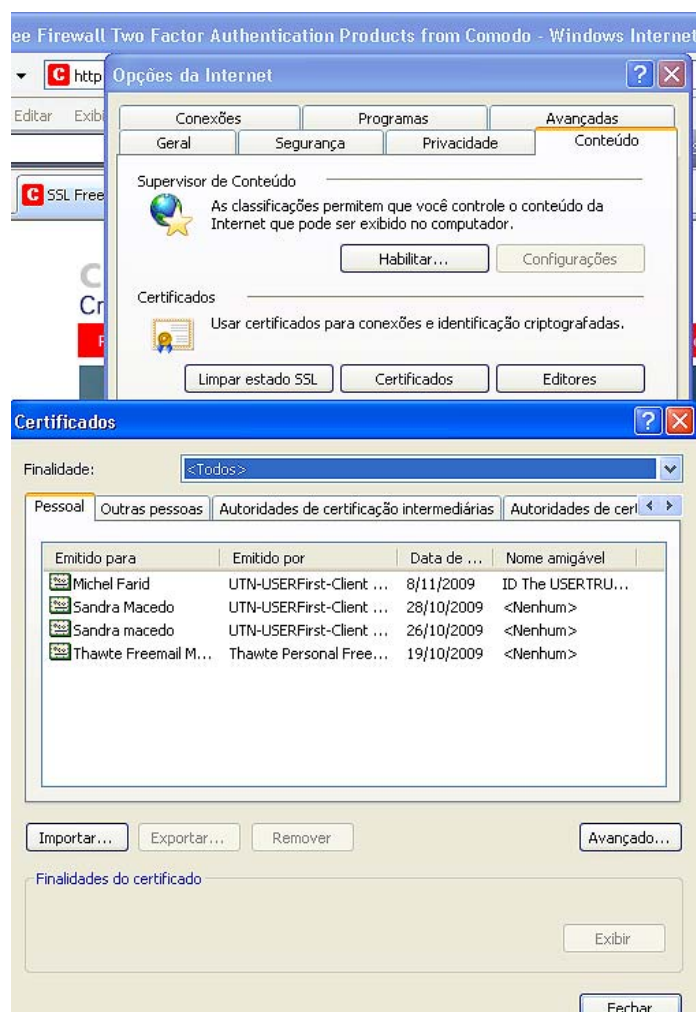


Figura 4.3-D: Lista dos certificados válidos

4.4 Como utilizar os certificados

Após a instalação do certificado no gerenciador de *emails*, o usuário poderá observar que ao enviar mensagens, estarão disponíveis dois novos itens na barra de ferramentas. Observe os botões “Assinar” e “Criptografar” na barra de ferramentas da mensagem na Figura 4.4. Ao serem acionados, são apresentados os ícones na direita dos campos “De” e “Para” indicando que esta mensagem será enviada assinada digitalmente e criptografada.

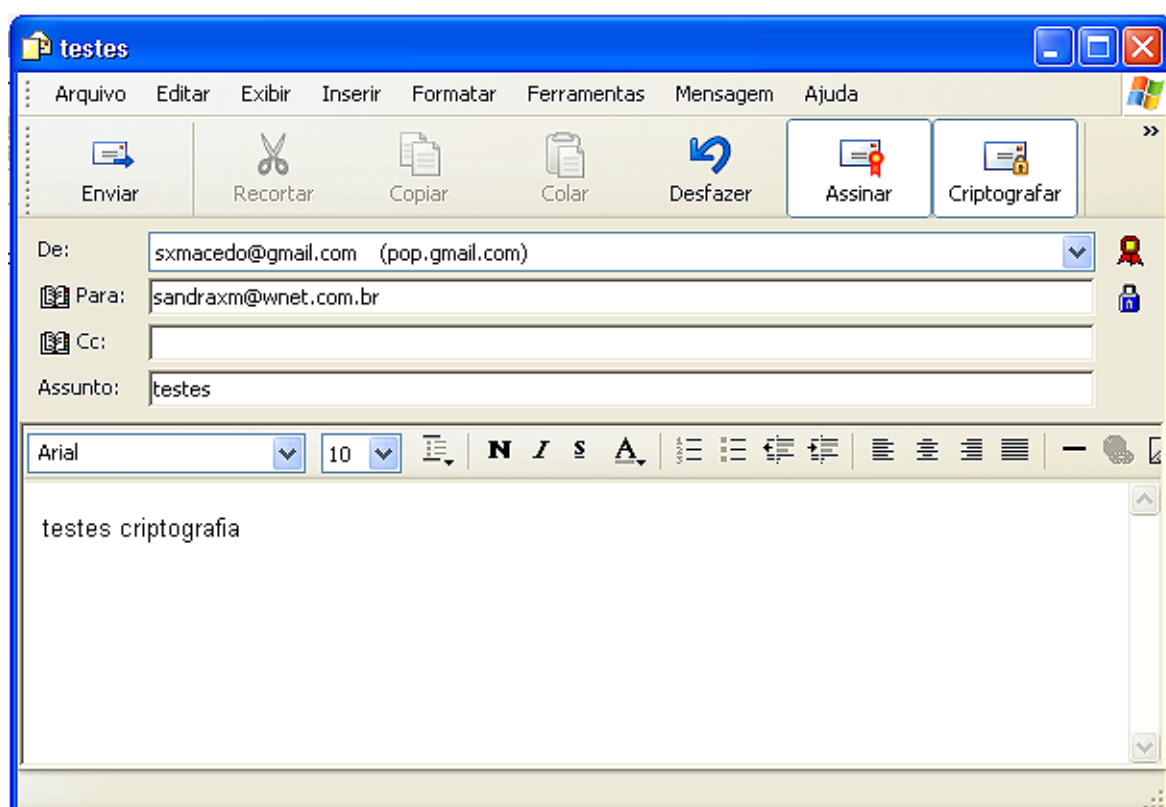


Figura 4.4: Envio de mensagem assinada digitalmente e criptografada.

Na Figura 4.4-A, pode-se visualizar o envio de mensagem com disponibilidade de certificado de *email* no *Microsoft Outlook 2007*.

Observe também que não são apresentados os ícones à direita dos campos ao acionar os botões de assinatura digital e criptografia. Isso é uma particularidade de cada gerenciador de *email*.

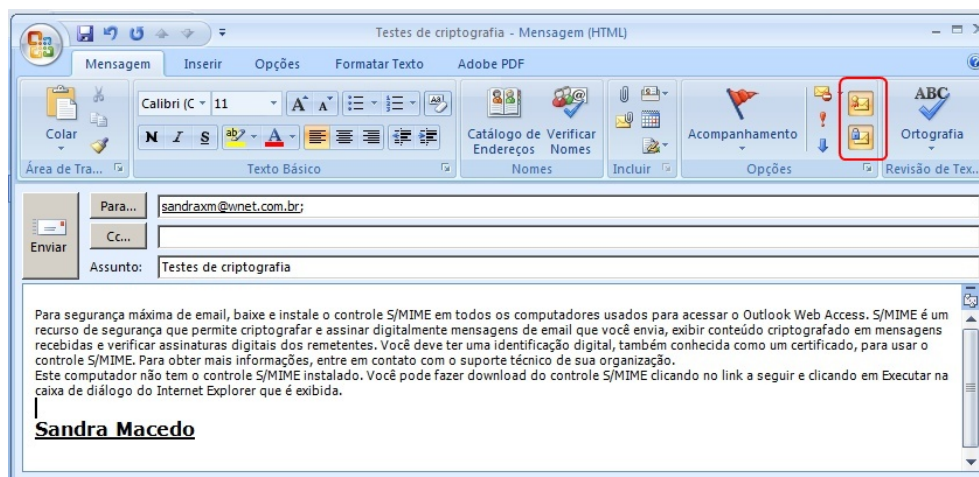


Figura 4.4-A: Certificado de *email* em mensagens no *Microsoft Outlook 2007*.

O gerenciador de *email* permite que se configure o envio da assinatura digital e/ou criptografia em todas as mensagens automaticamente. Porém podemos configurar também para que utilizemos estes botões de assinatura digital e criptografia quando desejarmos. Na Figura 4.4-B podemos ver uma mensagem criptografada recebida no gerenciador de *email*. Observe que ela está assinalada com um ícone específico de criptografia, um cadeado. A criptografia não permite que o conteúdo da mensagem seja visível no painel de leitura.

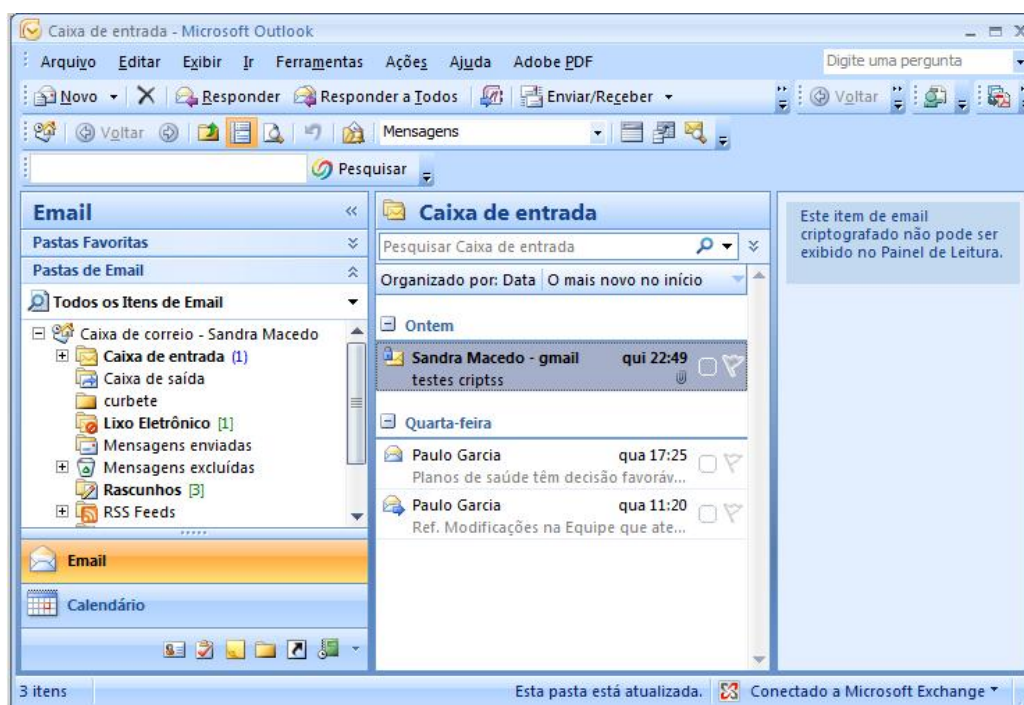


Figura 4.4-B: Mensagem criptografada recebida.

Como esta mensagem foi recebida pelo destinatário que possui a chave pública do remetente, a mensagem poderá ser visualizada normalmente logo ao ser aberta. Para que seja possível trocar mensagens criptografadas, é necessário que tenhamos a chave pública do destinatário, caso contrário, o gerenciador de *email* não permitirá o envio da mensagem com a criptografia. A assinatura digital independe desse detalhe, ou seja, é possível enviar mensagens com a assinatura digital para qualquer destinatário.

4.5 – Trocando Chaves Públicas

Os certificados de *email* podem ser utilizados para enviar uma mensagem assinada digitalmente, mas sem criptografia, o que garante ao remetente e ao destinatário saber se houve alguma violação da mesma. Ao receber uma mensagem assinada digitalmente é possível incluir o certificado do remetente clicando sobre a mensagem, propriedades, segurança, exibir certificados e clicar no botão “Adicionar ao catálogo de endereços”. Também é possível utilizar a opção de copiar o certificado recebido na mensagem para um arquivo clicando em “Certificado do remetente” e em seguida, na aba Detalhes e então no botão “Copiar para arquivo” conforme a Figura 4.5.

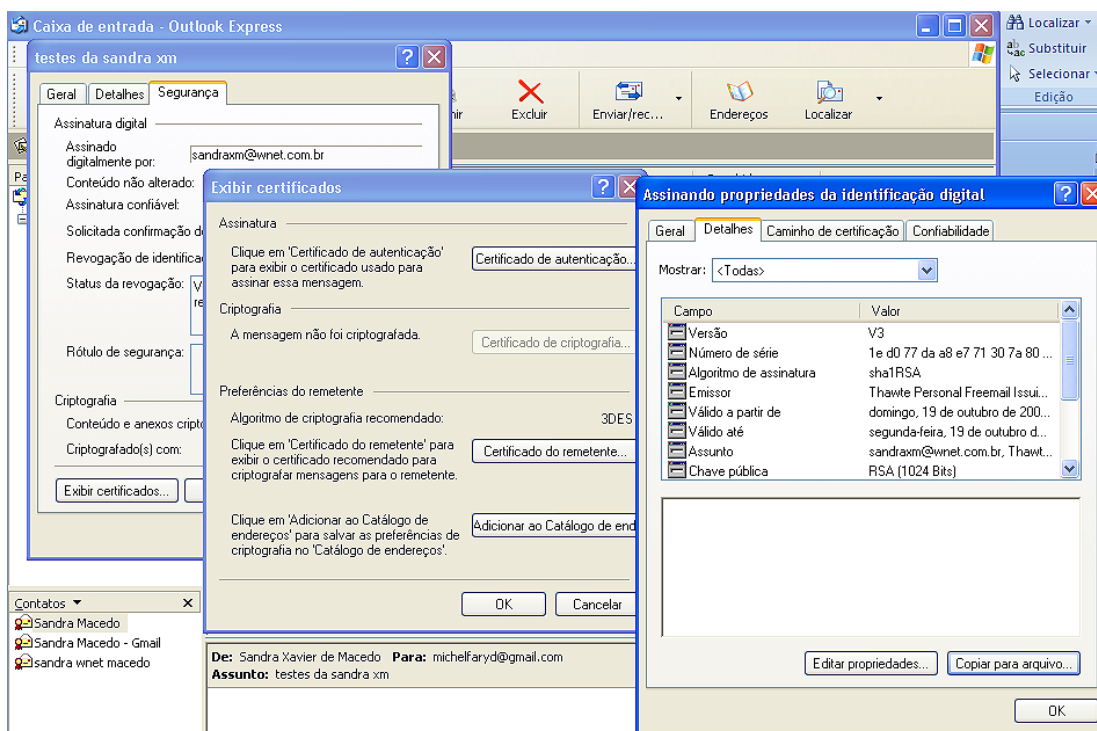


Figura 4.5: Copiando o certificado do remetente.

Para enviar ou receber mensagens criptografadas, é necessário ter as chaves públicas trocadas entre o destinatário e remetente da mensagem. Desta forma, o arquivo com a chave do usuário deverá ser exportado acessando as propriedades da conta do usuário, segurança, em preferências de criptografia, clique em selecionar, exibir certificado, aba detalhes e copiar para arquivo. Observe a Figura 4.5-A que exemplifica este procedimento:

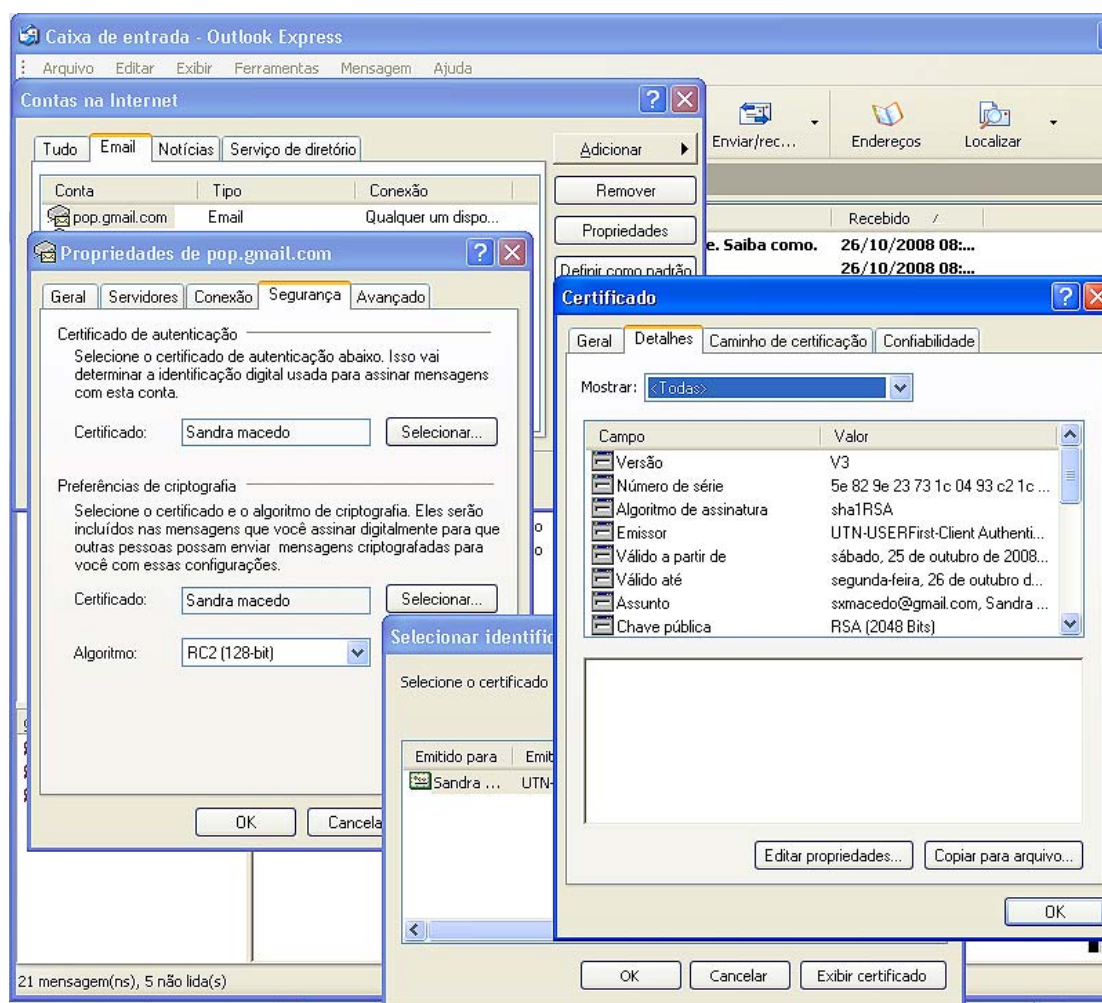


Figura 4.5-A: Copiando o certificado para gerar a chave pública.

Um assistente para a exportação será executado, bastando seguir os passos sugeridos. Um nome para a chave pública será solicitado. Observe o local no qual será armazenada a chave para poder encaminhá-la para o destinatário que se deseja compartilhar o recurso de criptografia.

Ao receber uma chave pública, basta fazer a importação da mesma para o contato de *email*.

No *Outlook Express*, acesse o catálogo de endereços;

Passo 1: Selecione o contato e clique em propriedades;

Passo 2: Selecione a aba “Identificações Digitais”;

Passo 3: Clique em “Importar” e localize o arquivo recebido, clique em Abrir e confirme a mensagem de alerta.

Após esse procedimento, é possível enviar e receber mensagens criptografadas.

5. PROTOCOLO SSL

Neste capítulo será abordado o protocolo SSL e como obter um certificado SSL.

Com o aumento das transações financeiras na *WEB*, surgiu uma necessidade maior de segurança dos dados trafegados. Isso é sentido tanto pelo internauta que expõe seus dados pessoais para efetivarem uma transação bancária, financeira, fiscal ou uma simples compra, quanto para o dono do site que se preocupa em disponibilizar segurança para o seu cliente.

Para suprir essa necessidade surgiu o protocolo SSL que possui um mecanismo que possibilita o sigilo absoluto dos dados e a garantia de autenticidade dos mesmos nas transações eletrônicas on-line.

5.1. Identificando um site seguro

Uma das maiores dificuldades para compras pela internet é a segurança dos dados informados no site e como saber se este site visitado é seguro ou não.

O SSL (*Secure Sockets Layer*) é utilizado para garantir a segurança no tráfego (troca) de informações sigilosas entre o usuário (*browser*) e um site (Servidor Web). Este processo é feito utilizando criptografia dos dados, prevenindo que os dados trafegados possam ser capturados ou mesmo alterados durante o seu curso entre o navegador do usuário e o site que ele está acessando. Por ser compatível com a maioria dos navegadores web, ele é muito utilizado.

Quando o site utiliza o protocolo SSL, ou seja, quando é um site seguro, poderá ser notado na barra de endereços o protocolo “https://” e não o usual “http://”. Além disso, também é exibido um cadeado à direita da barra de endereços na maioria dos browsers, indicando que os dados que ali forem digitados não serão interceptados ou modificados durante seu trajeto.

É possível observar estes detalhes no exemplo do site de assinaturas da Editora Abril demonstrado na figura a seguir:

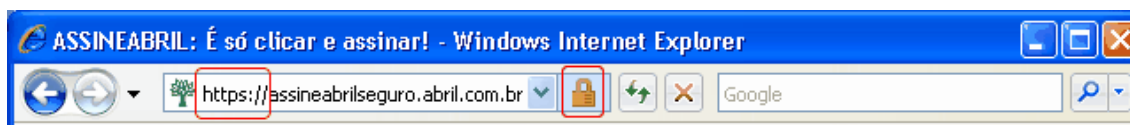


Figura 5.1: Barra de endereço seguro.

5.2 Características do SSL.

O protocolo SSL (*Secure Sockets Layer*) foi criado em 1994 pela Netscape Corporation, e desde a sua concepção tem-se tornado padrão devido a sua estrutura de fácil adaptação aos outros protocolos dentre os quais destaca-se o TCP-IP por ser o mais utilizado. A cada dia surgem novas necessidades de segurança para estas transações online e devido a isso, o protocolo SSL recebe novos mecanismos de segurança além da sua forma pura de criptografia. A Figura 5.2 demonstra as camadas na pilha de protocolos utilizando o SSL.



Figura 5.2: SSL e a pilha de protocolos TCP/IP

- **Segurança em conexões cliente/servidor**

O SSL, segundo Sousa e Puttini (2008), faz uso de criptografia simétrica garantindo o sigilo dos dados trocados entre as partes envolvidas na conexão. É adicionado um MAC (*Message Authentication Code*) em todas as mensagens, a fim de evitar que as mesmas, apesar de decifradas, sejam modificadas e com isso um ataque de escuta ativa seja possível. O MAC é calculado a partir de funções de *hash* seguras, garantindo a integridade das mensagens trocadas. Além de sigilo e integridade, o SSL ainda faz a autenticação das partes envolvidas para garantir e verificar a identidade das mesmas, utilizando criptografia assimétrica e certificados digitais.

- **Independência de protocolo**

O SSL roda sobre qualquer outro protocolo de transporte confiável, mas suas implementações são direcionadas para as redes com o protocolo TCP-IP por ser o mais utilizado.

- **Interoperabilidade**

Permite a comunicação com outra aplicação sem a necessidade do detalhamento de sua implementação;

- **Extensibilidade**

Admite a criação de novas rotinas e funcionalidades baseadas em mecanismos pré-existentes do protocolo. Temos como exemplo, a incorporação de novos parâmetros e métodos de criptografia (assimétrica ou simétrica) ao SSL sem que seja necessário implementar uma nova biblioteca ou mesmo criar um novo protocolo.

- **Eficiência**

O protocolo SSL dispõe da opção de armazenamento em cache de informações referentes à sessão, diminuindo o esforço computacional em sucessivas conexões. Isto o torna eficiente devido à demanda por recursos computacionais que este tipo de operação requer.

Vantagens do SSL

O SSL preenche todos os critérios necessários para transmissões das informações mais sigilosas, como dados pessoais e números do cartão de crédito. As aplicações podem optar por utilizar todos ou somente uma parte desses critérios dependendo do tipo e natureza das transações que estão sendo efetuadas.

5.3 Camadas do SSL

O protocolo SSL está dividido em duas camadas, a camada *Record* e a camada *Handshake*.

A camada ***Record*** é a de mais baixo nível, que interage com o protocolo de transporte. Ela é responsável por encapsular os dados das camadas superiores em pacotes compactados e cifrados e repassá-los para a camada de transporte.

A camada *Record* recebe as informações e as organiza em blocos numerados sequencialmente. É feita a compressão destes blocos seguida da geração de códigos de

autenticação MAC. Estes blocos são encriptados pelos algoritmos e chaves definidos pelo processo de *Handshake*, e enviados a seguir. A numeração destas informações é importante para que o receptor possa detectar se há blocos em falta, alterados ou injetados por terceiros. A figura 5.3 apresenta em destaque as camadas Record e Handshake no protocolo SSL.

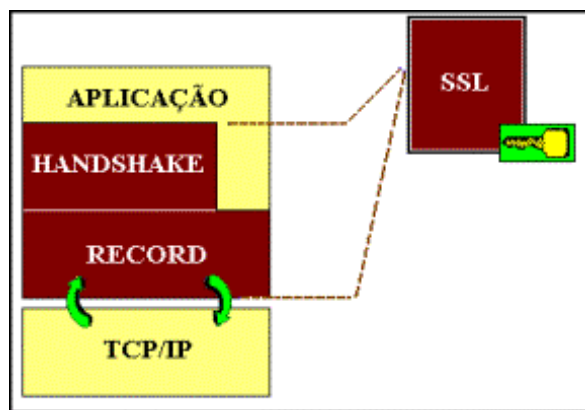


Figura 5.3: Camadas do Protocolo SSL (SOUSA e PUTTINI, 2008)

A camada *Handshake* está entre as camadas superiores e estabelece os parâmetros criptográficos da sessão. Ela permite que a aplicação servidora e a aplicação cliente autentiquem-se e negociem os algoritmos de cifragem e as chaves criptográficas antes que o protocolo de aplicação receba ou envie a informação (seu primeiro byte).

5.4 Processos no SSL

No SSL são executados 3 processos: Fragmentação, Compactação e Cifragem nesta ordem respectivamente.

5.4.1 Processo de Fragmentação

Neste processo, os dados originados das camadas de Aplicação e de *Handshake* são fragmentados em blocos de 214 bytes no máximo, e empacotados gerando uma *SSLPlainText*. Essa *SSLPlainText* contém o bloco de dados e a informação sobre o tipo destes dados, como a origem dos mesmos, ou seja, se são dados originados da camada de Aplicação ou de protocolos da camada *Handshake*.

5.4.2 Processo de Compactação

No processo de Compactação, os resultados do processo anterior (fragmentação) são compactados. Na versão atual do SSL, todas as implementações devem aceitar o tipo de compactação *Compression Method Null* que não realiza modificações nos dados. O resultado do processo de Compactação é o pacote *SSLCompressed*. Nele, o tamanho do bloco de dados não pode ser maior que 214 + 1024 bytes.

O processo de Compactação também é responsável pelo processo de descompactação dos pacotes resultantes do processo de decifragem, pois ele deve assegurar que os dados após a descompactação não causem estouro de buffer. Ocorrerá erro toda vez que o tamanho do bloco de dados ultrapassar 214 bytes após sua descompactação.

5.4.3 Processo de Cifragem

A Cifragem é o principal processo da camada *Record*. Ele é responsável por proteger os dados trafegados utilizando cifras e códigos MAC (*Message Authentication Code*). Na camada *Record*, os MACs têm uma característica adicional, um segredo que garante que o resultado do hash não poderá ser forjado por outro diferente daquele que conhece o segredo. O resultado do processo de cifragem é um pacote *SSLCipherText* que deverá ser enviado pela rede para o outro lado da comunicação.

5.5 Sessões no SSL

No SSL, o responsável pelos processos de troca de chaves, autenticação e estabelecimento de chaves de sessão é a camada *Handshake*. Nela são encontrados os protocolos ***Handshake***, ***ChangeCipherSpec (CSS)*** e o ***Alert***. Cada um destes protocolos tem um papel distinto durante os processos de Fragmentação, Compactação e Cifragem.

É importante esclarecer o conceito de Sessão no SSL. Uma sessão SSL é composta por um conjunto de dados que são gerados após um processo de *Handshake* completo.

Uma sessão é dada como sendo dependente do estado. O protocolo *Handshake* é quem mantém a consistência dos estados de uma sessão tanto no cliente quanto no servidor. Uma mesma sessão SSL pode incluir várias conexões, ou seja, a partir dos mesmos dados que formam uma sessão é possível abrir múltiplas conexões SSL (SOUSA e PUTTINI, 2008).

Os dados que compõem uma sessão são:

- ***session ID*** - um valor arbitrário escolhido pelo servidor para identificar esta sessão;
- ***peer certificate*** - usado para certificar uma organização. Está no formato X.509 e dentre outras coisas encontra-se dentro dele a chave pública da entidade que está utilizando aquela aplicação;
- ***compression method*** - algoritmo usado na compressão dos dados;
- ***cipherspec*** - especifica que conjunto de algoritmos de cifragem e de hash serão utilizados;
- ***Mastersecret*** - um segredo de 48 bytes compartilhado pelo servidor e pelo cliente;
- ***IsResumable*** - flag utilizado para indicar se a sessão pode ou não ser retomada ao iniciar uma nova conexão.

5.5.1 Protocolo *Alert*

Este protocolo faz o tratamento de erros. No SSL é enviada uma mensagem de erro para o outro lado da conexão sempre que ocorre um erro, e em alguns casos a conexão é abortada. Como o tratamento das mensagens de alerta são tratadas como normais, estas sofrem compactação e cifragem. Os níveis das mensagens de alerta são *warnings* e *fatals*. Os *warnings* apenas informam que alguma coisa anormal aconteceu ou foi detectada. Estes tipos de alertas em algumas versões do SSL, conforme foram implementados, podem gerar um fechamento da conexão. Quando os alertas forem fatais, a conexão será fechada, pois se referem ao comprometimento de algum segredo ou detecção de alguma falha durante a conexão. Todos os dados a respeito de uma sessão devem ser apagados, invalidando a sessão, quando um erro fatal é enviado ou recebido durante uma conexão.

As mensagens de alertas suportadas pela versão atual do protocolo SSL são:

- *close_notify: warning*, sinaliza o fechamento de uma conexão SSL;
- *unexpected_message*: fatal, indica o recebimento de uma mensagem fora de ordem;
- *bad_Record_mac*: fatal, indica que a verificação do MAC da mensagem recebida não coincidiu;
- *decompression_failure*: fatal, indica que o processo de descompactação resultou num bloco maior que 214 bytes;
- *Handshake_failure*: fatal, indica algum problema na negociação das informações de segurança;
- *no_certificate*: indica que o cliente não possui nenhum certificado que coincida com os tipos pedidos;
- *bad_certificate*: indica que o certificado recebido possui uma assinatura não válida;
- *unsupported_certificate*: indica recepção de certificado cujo o tipo não é suportado;
- *certificate_revoked*: indica que o certificado foi revogado por quem o assinou;
- *certificate_expired*: indica que a data de validade do certificado expirou ou, de que este ainda não está válido;
- *certificate_unknown*: indica qualquer outro problema relacionado com falhas no certificado;
- *illegal_parameter: fatal*, indica que algum campo de alguma mensagem trafegada durante o *Handshake* está fora do seu intervalo ou incoerente com outro campo.

5.5.2 Protocolo ChangeCipherSpec

Segundo Sousa e Puttini (2008), este protocolo é formado por uma única mensagem, a *change_cipher_spec*. Sua função é sinalizar alguma modificação nas estratégias ou parâmetros de segurança utilizados. Quando uma das partes do protocolo recebe uma mensagem *change_cipher_spec* durante o processo de *Handshake*, ela automaticamente troca as informações do estado corrente de leitura (estratégia atual) pelos dados do estado pendente de leitura (estratégia recém negociada). Porém, quando uma das partes envia uma *change_cipher_spec*, ela automaticamente deve atualizar seu estado corrente de escrita para o estado pendente de escrita. Qualquer mensagem enviada ou recebida após esta mensagem será trabalhada utilizando a nova estratégia de segurança, negociada no processo de *Handshake*. Esta mensagem sempre precederá a mensagem de *FINISHED*. Uma mensagem *change_cipher_spec* inesperada ocasiona o envio de um alerta *unexpected_message*.

5.5.3 Protocolo *Handshake*

O Protocolo *Handshake* é a principal parte do SSL. Ele é constituído por duas fases.

1. Na primeira, é feita a escolha da chave entre o cliente e o servidor, a autenticação do servidor e a troca da chave Master.
2. Na segunda, é feita a autenticação do cliente (se requerida) e o fim do *Handshake*.

Após o *Handshake* estar completo, a transferência de dados entre aplicações poderá ser iniciada. As mensagens do protocolo *Handshake* seguem o formato da Figura 5.5.3, onde:

Handshake-Type: indica o tipo de mensagem de *Handshake* sendo enviada;

Tamanho: é o tamanho do corpo em bytes;

Corpo: são os dados da mensagem sendo enviada.

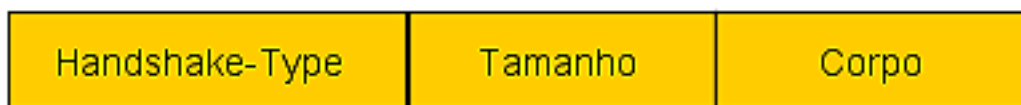


Figura 5.5.3 – Formato da mensagem do protocolo *Handshake*

5.6 Como Gerar um Certificado SSL

Um certificado SSL é requisitado para a utilização em *websites* para garantir a proteção dos dados informados no mesmo. Para obtê-lo, o responsável pelo *website* deve fornecer informações tais como endereço, documentação e pessoa de contato. À partir desses dados é gerado um par de chaves de criptografia para a codificação dos dados sendo uma chave privada e outra chave pública. A privada ficará no servidor e a pública juntamente com as informações cadastrais, será utilizada para gerar um CSR (*Certificate Signing Request*).

O CSR é submetido a uma Autoridade Certificadora (CA) que validará os dados cadastrais comprovando sua autenticidade bem como a propriedade do *website*, garantindo que aquele certificado foi realmente emitido para o proprietário do *website*.

Após a Autoridade Certificadora gerar o certificado, este deverá ser instalado pelo provedor responsável pela hospedagem do *website*.

Segundo consta no site da Laniway, para a escolha de um certificado apropriado deve-se observar se este é reconhecido pela maioria dos navegadores. Caso este problema ocorra, o acesso ao *website* pode ficar comprometido devido às mensagens de alerta de incompatibilidades que aparecerão durante os acessos. Para evitar isso, é importante procurar um certificado de uma Autoridade Certificadora de renome no mercado e que tenha a aprovação dos usuários que a utilizam, e também dos desenvolvedores dos navegadores. É indicado usar um certificado a partir de 128 de bits de codificação para maior segurança nas informações trafegadas.

6. QUESTÕES TÉCNICAS ENVOLVIDAS NA CERTIFICAÇÃO DIGITAL

Neste capítulo será abordada a parte técnica que envolve a certificação digital como a utilização de criptografias, quais os tipos de criptografia utilizados, alguns dos algoritmos mais utilizados e o conceito e utilização de chaves públicas e privadas.

6.1. Criptografia

A palavra CRIPTOGRAFIA tem origem das palavras gregas *kryptós* que significa “oculto” e *graph* que significa “escrever”. Segundo Silva *et al* (2008), “Criptografia é a ciência de fazer com que o custo de adquirir uma informação de maneira imprópria seja maior do que o custo obtido com a informação”.

A criptografia deve seguir quatro princípios básicos:

- 1) Confidencialidade;
- 2) Autenticação;
- 3) Integridade da informação e
- 4) Não repudiabilidade (o remetente não pode negar o envio da informação).

Alguns conceitos são importantes no processo da criptografia.

- **Criptosistemas**

Fornecem técnicas para cifrar ou embaralhar textos. Estes textos quando cifrados, tornam-se aparentemente ilegíveis, sendo posteriormente obtida sua forma original e legível. O texto original é chamado de “texto pleno” ou “texto claro” e o texto ilegível é conhecido como “texto cifrado”.

- **Encriptamento ou Encriptação**

É o processo de “embaralhar” ou “cifrar” textos ou mensagens, sendo o processo inverso denominado descriptamento ou descriptação. O encriptamento baseia-se em dois componentes básicos: um algoritmo e uma chave.

- **Algoritmos Criptográficos**

É a função matemática que identifica os passos de encriptação ou descriptação.

Os criptosistemas são baseados em apenas três tipos de algoritmos criptográficos: chave secreta, chave pública e resumo.

6.2. Tipos de Criptografias

No início, a criptografia era feita utilizando apenas um algoritmo para cifrá-la e o mesmo para decifrá-la. Esse método era inseguro, pois um intruso poderia acessar a informação além do receptor bastando para isso ter conhecimento do algoritmo utilizado.

Para solucionar este problema, iniciou-se o uso de chaves empregadas ao algoritmo. Dessa forma, pode-se usar o mesmo algoritmo para vários receptores, utilizando-se chaves diferentes para cada um (ALECRIM, 2005).

Os termos “chave de 8 bits”, “chave de 64 bits”, “chaves de 128 bits” e assim por diante, expressam o tamanho da chave. Esse tamanho é calculado elevando 2 à potência do número de bits, para uma chave de 8 bits (2^8 elevado a potência 8), por exemplo, pode-se ter 256 combinações de chaves geradas. Para 128 bits o número de combinações certamente é muito maior, portanto a segurança é proporcionalmente maior.

Na criptografia, os algoritmos clássicos, de acordo com a chave que utiliza, podem ser simétricos (ou de chave privada) ou assimétricos (ou de chave pública):

6.2.1 Algoritmos Simétricos ou de Chave Privada

Utilizam a mesma chave para criptografar e decriptar uma mensagem sendo que para isso, as duas partes envolvidas na comunicação devem ter a mesma chave secreta.

O processo de criptografia para chaves simétricas está presente nos seguintes algoritmos de encriptação:

DES (*Data Encryption Standard*)

Este algoritmo utiliza um sistema de cifragem em blocos. Foi criado em 1977 pela IBM e permite cerca de 72 quadrilhões de combinações, mas seu tamanho de chave (56 bits) é considerado pequeno, tendo sido quebrado por "força bruta" em 1997 em um desafio lançado na Internet (PORTAL ICP-BRASIL, 2008) .

IDEA (*International Data Encryption Algorithm*)

O IDEA é o algoritmo para criptografia de *email* pessoal mais disseminado no mundo. Seu tamanho de chave é de 128 bits. Foi criado em 1991 por *James Massey* e *Xuejia Lai* e é estruturado de forma semelhante ao DES, mas na maioria dos microprocessadores, uma implementação por software do IDEA é mais rápida do que uma implementação por software do DES (PORTAL ICP-BRASIL, 2008).

RC (*Ron's Code ou Rivest Cipher*)

Este algoritmo, criado por *Ron Rivest* na empresa *RSA Data Security*, é muito utilizado em e-mails e faz uso de chaves que vão de 8 a 1024 bits. Possui várias versões: RC2, RC4, RC5 e RC6 diferenciando-se entre elas pelo tamanho das chaves.

Podemos citar alguns outros algoritmos conhecidos, como o AES (*Advanced Encryption Standard*), baseado no DES, o 3DES, o *Twofish*, outros (ALECRIM, 2008).

6.2.2 Algoritmos Assimétricos ou de Chave Pública

Utilizam duas chaves no processo: a chave pública para criptografar a mensagem, e a chave privada para decriptar, não havendo troca de chaves. Seu exemplo mais conhecido é o RSA.

RSA – É o método de criptografia de chave pública mais utilizado. Ele foi inventado em 1978 por *Rivest*, *Shamir* e *Adleman*, que então trabalhavam no *Massachussets Institute of*

Technology (M.T.I). Este algoritmo é baseado na multiplicação de dois número primos resultando num terceiro valor que corresponde à chave privada. A chave pública é composta pelos dois números primos que foram multiplicados.

ElGamal – Criado por *Taher ElGamal*, é freqüente em assinaturas digitais. Este algoritmo garante a autenticidade da mensagem mesmo em canais não seguros, fazendo uso do problema de logaritmo de algoritmo discreto. A geração de chaves segue o padrão das chaves públicas, onde cada entidade gera um par de chaves e acertam a forma como vão distribuir as chaves públicas.

6.2.3 Função Hashing

Esta função é utilizada como componente em assinaturas digitais devido à lentidão dos algoritmos assimétricos que são em torno de 1.000 vezes mais lentos do que os simétricos. A função *Hashing* gera um valor pequeno, de tamanho fixo da mensagem que se quer assinar independente do seu tamanho. Desta forma, essa função torna as assinaturas digitais ágeis e confiáveis. A função *Hashing* também é chamada de *Message Digest*, *One-Way Hash Function*, Função de Condensação ou Função de Espalhamento Unidirecional. Ela funciona como uma impressão digital de uma mensagem gerando um valor pequeno denominado “*digest*” ou “*valor hash*”, a partir de uma entrada de tamanho variável. Esses valores e sua relação com a mensagem podem ser comparados com a conta-corrente e sua relação com o dígito verificador. Portanto servem para garantir a integridade do conteúdo da mensagem que representam. Após o cálculo do valor *hash* por uma função *Hashing*, caso haja alguma alteração no conteúdo da mensagem, esta alteração será detectada, pois um novo cálculo resultaria em um valor *hash* diferente. A seguir são descritas algumas das funções que utilizam o cálculo do valor *hash*.

- Função MD5 - É uma função de espalhamento unidirecional. A sigla MD significa *Message Digest*. Ela produz um valor *hash* de 128 bits.
- Função SHA-1 – *Secure Hash Algorithm* também é uma função de espalhamento unidirecional. Gera um valor *hash* de 160 bits. Até então, não é conhecido nenhum ataque de criptoanálise contra o SHA-1 embora não se possa afirmar que não ocorra no futuro.

6.2.4 Criptografia Quântica

A criptografia quântica é um dos mais recentes métodos de criptografia e embora já seja comum no meio científico, ela engloba apenas a troca segura de chaves, utilizando princípios da Mecânica Quântica, ou seja, a natureza quântica dos fótons. Desta forma, ainda é necessária a utilização da criptografia clássica. A criptografia quântica também é conhecida como “Distribuição Quântica de Chaves ou QKD (*Quantum Key Distribution*), e ela difere dos demais métodos criptográficos porque não precisa do segredo nem do contato prévio entre as partes. Ela é considerada altamente segura, porém de custo de implantação elevado (PC WORLD, 2007).

6.2.5 Criptografia nas Redes Sem Fio

Com algum conhecimento técnico, os dados podem ser facilmente interceptados em redes wireless devido a brechas na segurança dos dados trafegados. Em face destes problemas, houve uma grande necessidade de se desenvolver técnicas de criptografias apropriadas, tornando esse tipo de comunicação viável tanto no meio empresarial quanto para usuários domésticos.

Os tipos de criptografia mais usados nas redes wireless são:

WEP (*Wired Equivalent Privacy*) – Utiliza uma chave secreta compartilhada e o algoritmo RC4 para criptografia. Segundo Santos Jr. (2008), o WEP foi o primeiro padrão de segurança para redes wireless. Além do RC4, seu algoritmo utiliza um gerador de número pseudo-randômico (*PRGN-Pseudo Number Random Generator*). Uma das vantagens dele é a rapidez para criptografar e descriptografar economizando muitos ciclos de CPU além da facilidade para ser implementado. Pela sua simplicidade, este algoritmo foi quebrado em 1996.

WPA (*WI-FI Protected Access*) e **WPA2**, ambas são baseadas no protocolo *Wi-Fi Alliance* para redes locais sem fio, sendo utilizadas por empresas e em redes domésticas. A WPA2 é considerada a próxima geração de segurança *Wi-Fi*. Atualmente são utilizadas por vários órgãos governamentais no mundo todo.

6.3 Pontos Falhos na Criptografia

A Criptografia Clássica possui alguns pontos falhos em relação ao uso de chaves:

- 1) Nos algoritmos de chave simétrica, existe o problema de se manter um canal seguro para a troca de chaves, não podendo detectar um possível espião que poderia copiar a chave transmitida.
- 2) Já os algoritmos de chave assimétricos, têm sua segurança baseada numa pretensa intratabilidade computacional pelo fato de que os algoritmos de fatoração para os computadores atuais são de ordem exponencial, o que praticamente invalida a quebra do protocolo. Porém, segundo *Shor*, citado por OLIVEIRA (2008), a fatorização de números pode ser feita em tempo polinomial num computador quântico, o que coloca em xeque a segurança desses sistemas criptográficos.
- 3) Nos algoritmos de chaves assimétricas, a segurança é baseada em fatoração de números com resultados exponenciais, tornando assim difícil a violação, porém com a aplicação da computação quântica que torna possível essa fatoração muito mais rápida que a computação clássica, segundo *Shor*, citado por OLIVEIRA (2008), no dia em que um computador quântico for ligado, nenhuma mensagem criptografada classicamente será secreta.
- 4) Em qualquer dos métodos é impossível saber classicamente se há alguém monitorando o canal de comunicação. Uma saída para esses problemas é encontrada na Criptografia Quântica cuja segurança é baseada nas leis da Física Quântica, e promete que se alguém interceptar a troca de chaves será possível detectar sua presença, e se as chaves são usadas no método *One-Time Pad*, então é obtida a segurança completa.

CONSIDERAÇÕES FINAIS

A segurança na Web pode ser obtida desde que aplicadas às devidas medidas para tal objetivo. A falta de conhecimento de como utilizar e quais as ferramentas utilizar, deixam várias pessoas fora da rede, ou seja, da web, por serem temerosas com os perigos de fraudes existentes no mundo virtual, ou mesmo a invasão de privacidade.

A MP 2200-2, criada em agosto de 2001, define toda a cadeia da certificação no Brasil e a função de cada órgão dentro desta cadeia.

Podemos observar que a implantação da criptografia para a proteção de mensagens eletrônicas (emails) é simples e existem sistemas gratuitos que disponibilizam tal serviço, mas na sua maioria são empresas estrangeiras. Também existe a necessidade da utilização de softwares gerenciadores de emails para configurar as chaves de criptografia.

Existem 8 tipos de certificados no Brasil, sendo 4 deles para uso em assinaturas digitais e 4 para a codificação de documentos, base de dados e outras informações sigilosas. Atualmente no Brasil, o tipo de certificado para assinatura digital A3 é o mais procurado devido à segurança que o mesmo proporciona, a facilidade de configuração e de uso, e o custo/benefício.

O protocolo SSL é mundialmente o mais utilizado para a segurança na troca de informações entre *websites*. Ele é facilmente adaptável à maioria dos protocolos, entre os quais se destaca o TCP-IP que é o mais utilizado. Devido a esse fato, a maioria das implementações do SSL são feitas visando a utilização com o TCP-IP, mas mantendo sempre a característica de adaptabilidade aos demais protocolos.

No futuro, a segurança na rede tende a ser cada vez mais aprimorada e versátil dando oportunidades cada vez maiores da disseminação da informação. Existe uma forte tendência à utilização da computação quântica, o que promete tornar a web e todos os sistemas informatizados mais seguros.

As redes wireless ganharam um espaço considerável e merecem especial atenção no que envolve a segurança.

TRABALHOS FUTUROS

No decorrer do desenvolvimento deste trabalho podemos vislumbrar algumas possibilidades de trabalhos futuros, tais como:

- Utilização da criptografia quântica.

Abordando seus princípios, mecanismo, histórico, como funciona a criptografia em relação aos algoritmos aplicados, exemplos de aplicações deste método de criptografia.

- Utilização da criptografia em redes wireless.

Detalhamento do funcionamento dessas criptografias, tipos de algoritmos criptográficos utilizados (WPA, WPA2 que são os mais recentes e mais usados), comparação com os demais métodos existentes.

REFERÊNCIAS

SILVA, Luiz Gustavo C., *et al.* **Certificação Digital - Conceitos e Aplicações**. 1 ed. Rio de Janeiro: Editora Ciência Moderna, 2008. 201p.

PRESIDÊNCIA DE REPÚBLICA-CASA CIVIL. **Medida Provisória N° 2.200-2, de 24 de agosto de 2001**, disponível em:

https://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm, Acessado em Nov.2008

INFOMONEY. **Certificação digital: saiba quanto custa e como obter seu e-CPF ou e-CNPJ**, disponível em: <http://dinheiro.br.msn.com/especiais/ir/artigo.aspx?cp-documentid=4139155>, Acessado em jul. 2008.

RIBEIRO, Gisele. **Como funciona o certificado digital**, disponível em:

<http://informatica.hsw.uol.com.br/certificado-digital7.htm>, Acessado em Nov. 2008.

AC-JUS, **Normas ICP-Brasil - Resolução 41 de 18 de Abril de 2006**, disponível em:

<https://www.gestao.acjus.gov.br/legislacao/icp-brasil>, Acessado em Nov.2008.

TORRES, Gabriel. **Smart Card**, disponível em:

<http://www.clubedohardware.com.br/artigos/665>, Acessado em set. 2008

COMODO- Authentic & Secure, **Free email secure certificate**, disponível em:

<HTTP://www.comodo.com>, Acessado em Out.2008.

MAIA, Luis Paulo; PAGLIUSI, Paulo Sérgio. **Criptografia e certificação digital**, disponível em: http://www.training.com.br/lpmaia/pub_seg_cripto.htm, Acessado em set. 2008.

GOMES, Rodrigo. **Conceitos de criptografia com chave simétrica e assimétrica**, disponível em: <http://www.vivaolinux.com.br/artigo/Conceitos-de-criptografia-com-chave-simetrica-e-assimetrica/?pagina=3>, Acessado em set. 2008.

ALECRIM, Emerson. **Criptografia**, disponível em:

<http://www.infowester.com/criptografia.php>, Acesso em set. 2008.

UNO, Daniel Nobuo, FALEIROS, Antônio Cândido. **Princípios de criptografia quântica**, disponível em: <http://www.bibl.ita.br/ixencia/artigos/FundDanielNobuo.pdf>, Acessado em Nov. 2008.

ITI. **ICP-BRASIL**, disponível em:

<http://www.iti.gov.br/twiki/bin/view/Certificacao/WebHome>, Acessado em Nov.2008.

ICP-BRASIL. **DES – Data encryption standard**, disponível em :

<https://www.icpbrasil.gov.br/duvidas/glossary/des-data-encryption-standard>, Acessado em set. 2008.

ICP-BRASIL. **IDEA – International data encryption algorithm**, disponível em :

<https://www.icpbrasil.gov.br/duvidas/glossary/idea-international-data-encryption-algorithm>, Acessado em set. 2008.

OLIVEIRA, Ivan S., **Computação quântica**, disponível em:

<http://www.comciencia.br/reportagens/nanotecnologia/nano16.htm>, Acessado em Nov.2008.

SANTOS JR, Arthur R. **O uso do WEP (Wired Equivalent Privacy)**, disponível em:

http://www.instonline.com.br/index2.php?option=com_content&do_pdf=1&id=54, Acessado em Nov.2008.

SOUSA Jr., Rafael T., PUTTINI, Ricardo. **SSL3.**, disponível em:

<http://www.redes.unb.br/security/ssl3/protocolo.html#protocolo>, Acessado em Set.2008.

LANIWAY, **Certificados seguros SSL**, disponível em:

<http://www.laniway.com.br/br/corporativo/certificado.do>, Acessado em Out.2008.