UNIÃO EDUCACIONAL MINAS GERAIS S/C LTDA.
FACULDADE DE CIÊNCIAS APLICADAS DE MINAS
Autorizada pela Portaria no 577/2000 - MEC, de 03/05/2000
ESPECIALIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

MINIMIZANDO OS SPAMS COM O USO DE E-MAILS SEGUROS

MÁRCIO AURÉLIO RIBEIRO MOREIRA

Uberlândia - MG - Brasil
2007

MÁRCIO AURÉLIO RIBEIRO MOREIRA

MINIMIZANDO OS SPAMS COM O USO DE E-MAILS SEGUROS

Monografia apresentada à Faculdade de Ciências Aplicadas de Minas Gerais da União Educacional Minas Gerais - UNIMINAS, como parte dos requisitos para obtenção do Título de Especialista em Segurança da Informação.

Orientador: Prof. M. Sc. Gilson Marques da Silva

Uberlândia - MG - Brasil

2007

MÁRCIO AURÉLIO RIBEIRO MOREIRA

MINIMIZANDO OS SPAMS COM O USO DE E-MAILS SEGUROS

Monografia apresentada à Faculdade de Ciências Aplicadas de Minas Gerais da União Educacional Minas Gerais - UNIMINAS, como parte dos requisitos para obtenção do Título de Especialista em Segurança da Informação.

Orientador: Prof. M. Sc. Gilson Marques da Silva

Banca Examinadora:

Uberlândia (MG), 6 de Outubro de 2007.

_____

Prof. M. Sc. Gilson Marques da Silva (Orientador)

_____

Prof. M. Sc. Alex Fabianne de Paulo - FPU

_____

Prof. Esp. Flamaryon Guerin Gomes Borges - Uniminas

Uberlândia - MG - Brasil

2007

Dedico este trabalho a meus pais, pela vida e pelo amor.

AGRADECIMENTOS

À minha querida esposa Cida pelo amor, compreensão das ausências e paciência durante o desenvolvimento deste trabalho. Aos meus queridos filhos Michele e Bruno pelo amor, por suportar as ausências, pelo incentivo e pela motivação.

Ao caríssimo professor e orientador Gilson Marques pelo exemplo, motivação, orientação, dedicação e paciência demonstrada durante todas as etapas deste trabalho. Aos amigos e professores Marcelo Pereira Cardoso e Luiz Carlos Goiabeira Rosa pelas inestimáveis orientações e sugestões jurídicas. Ao amigo Adalberto Minto Soncini pela revisão de parte do trabalho.

Aos professores da especialização pela dedicação, compreensão, apoio e troca de experiências que tivemos durante todo o curso. Aos companheiros de jornada pela motivação, companheirismo e cooperação com os quais fui brindado durante o curso.

A todos, que direta ou indiretamente contribuíram para mais esta realização em minha vida. Meus mais sinceros agradecimentos.

RESUMO

Os sistemas de correio eletrônico e, consequentemente, os e-mails vem se popularizando significativamente nos últimos anos. Para as empresas os e-mails tornaram-se também ferramentas de trabalho e de fechamento de negócios. Paralelamente os e-mails indesejados, conhecidos como *spams*, além de encherem as pessoas de informações indesejadas tornaram-se propagadores de vírus, vermes, correntes, etc. Este trabalho investiga formas de reduzir a geração de *spams*. A estratégia adotada baseia-se no fato que os *spammers* (emissores de *spam*) procuram ocultar suas identidades para não serem responsabilizados por seus atos. Logo, se a comunidade adotar os e-mails seguros (aqueles que possuem integridade, autenticidade e eventualmente confidencialidade), os *spammers* poderão ser responsabilizados por seus atos e consequentemente diminuirão a emissão de *spams*. Se esta adoção for simples, este caminho é inevitável. Inicialmente foi explorado o funcionamento dos sistemas de e-mail. Depois foram investigados os protocolos existentes atualmente (STMP, POP3, IMAP, S/MIME, SPF e DKIM), concluindo-se que o S/MIME é capaz de enviar e receber e-mails seguros. Diante disto, foi mostrado como utilizar o S/MIME nos sistemas de e-mails atuais. Finalmente, foi abordado o uso de e-mails como provas em questões judiciais.

Palavras chave: E-mails, e-mails seguros, spams, spammers, S/MIME, SPF e DKIM.

ABSTRACT

The electronic mail systems and consequently the e-mails became significantly popularized in the last years. For the companies, the e-mails are used as work tools and are used to make business. Parallel the undesirables e-mails, known as spam, besides to fill people with undesirable information became spreaders of virus, worms, chain letters, etc. This work investigates the ways of reducing the spam generation. The adopted strategy based on the fact that the spammers (spam originators) tries to hide their identities, so they can't be made responsible by their actions. Therefore, if the community adopts the safe e-mails (those with integrity, authenticity and eventually confidentiality), the spammers can be made responsible by their actions and consequently they will reduce the spam emission. If this adoption is simple, this way is inevitable. Initially, the e-mail systems operation was explored. So, the existent protocols (STMP, POP3, IMAP, S/MIME, SPF and DKIM) were investigated, this work concludes that S/MIME is capable to send and receive safe e-mails. After this, it was shown how to use S/MIME in the current e-mails systems. Finally, the use of e-mails was approached as proofs in judicial subjects.

Keywords: E-mails, safe e-mails, spam, spammers, S/MIME, SPF and DKIM.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SÍMBOLOS

ACL	*Access Control List* (lista de controle de acesso)
ADMD	*Administrative Management Domain* (gerenciamento administrativo de domínio)
ANOREG	Associação dos Notários e Registradores do Brasil
ASCII	*American Standard Code for Information Interchange* (código padrão americano para o intercâmbio de informações)
CA	*Certificate Authority* (autoridade certificadora)
CBC	*Cipher Block Chaining* (cifragem por encadeamento de blocos)
CEF	Caixa Econômica Federal
CertJUS	Certificado Digital do Poder Judiciário Brasileiro
CFB	*Cipher Feedback Mode* (cifragem pelo modo de feedbacks)
CGI	Comitê Gestor da Internet
CMS	*Cryptographic Message Syntax* (sintaxe de mensagens criptográficas)
DES	*Data Encryption Standard* (cifragem padrão de dados)
DKIM	*DomainKeys Identified Mail* (mensagens identificadas por domínio de chaves)
DMZ	*Demilitarized Zone* (zona desmilitarizada)
DOU	Diário Oficial da União
DSS	*Digital Signature Standard* (assinatura digital padrão)
e-CAC	Centro Virtual de Atendimento ao Contribuinte
e-CNPJ	Certificado Digital do Cadastro Nacional de Pessoas Jurídicas
e-CPF	Certificado Digital do Cadastro de Pessoas Físicas
EDE3	*Encrypt Decrypt Encrypt with Triple DES* (cifra-decifra-cifra com o triplo DES)
E-MAIL	*Electronic Mail* (mensagem eletrônica)
ESMTP	*Extended SMTP* (SMTP extendido)
FEBRABAN	Federação Brasileira de Bancos
FTC	*Federal Trade Commission* (Comissão Federal de Comércio do governo americano)
FTP	*File Transfer Protocol* (protocolo de transferência de arquivos)
HTTP	*Hyper Text Transfer Protocol* (protocolo de transferência de hipertexto)
HTTPS	*Hyper Text Transfer Protocol Secure* (protocolo seguro de transferência de hipertexto)
ICP-Brasil	Infra-Estrutura de Chaves Públicas Brasileira
IETF	*Internet Engineering Task Force* (força-tarefa de engenharia da Internet)
IIS	*Internet Information Services* (serviços de informações da Internet)
IMAP	*Internet Message Access Protocol* (protocolo de acesso a mensagens Internet)

IMESP	Imprensa Oficial do Estado S.A. (Imprensa Oficial do Estado de São Paulo)
IMS	*Identity Management System* (Sistema de Gerenciamento de Identidade)
IP	*Internet Protocol* (protocolo Internet)
ITI	Instituto Nacional de Tecnologia da Informação
LAN	*Local Area Network* (redes locais)
MAA	*Mail Access Agent* (agente de acesso a mensagens)
MDA	*Mail Delivery Agent* (agente de entrega de mensagens)
MIME	*Multipurpose Internet Mail Extensions* (extensões multi-propósito de mensagens Internet)
MIT	*Massachusetts Institute of Technology* (Instituto de Tecnologia de Massachusetts)
MOSS	*MIME Object Security Services* (serviços de segurança de objetos MIME)
MSA	*Mail Submission Agent* (agente de submissão de mensagens)
MTA	*Mail Transfer Agent* (agente de transferência de mensagens)
MUA	*Mail User Agent* (agente de mensagens do usuário)
NAT	*Network Address Translation* (tradução de endereços de rede)
PEM	*Privacy Enhanced Mail* (mensagens com privacidade melhorada)
PGP	*Pretty Good Privacy*
PKCS	*Public-Key Cryptography Standards* (padrões de criptografia de chave-pública)
PKI	*Public Key Infrastructure* (infra-estrutura de chave pública)
POP	*Post Office Protocol* (protocolo de agência postal)
POP3	*Post Office Protocol version 3* (versão 3 do protocolo de agência postal)
PRODEMG	Companhia de Processamento de Dados do Estado de Minas Gerais
RADIUS	*Remote Authentication Dial-In User Service* (serviço remoto de autenticação de usuários discados)
RFC	*Request for Comments* (requisição para comentários, documento padrão do IETF)
RSA	Marca registrada da empresa RSA Data Security, Inc. fundada por Ron **R**ivest, Adi **S**hamir e Len **A**dleman (três professores do MIT).
S/MIME	*Secure / Multipurpose Internet Mail Extensions* (extensões seguras multi-propósito de mensagens Internet)
SANS	*SysAdmin, Audit, Network, Security* (Instituto de Segurança, Rede, Auditoria e Administração de Sistemas)
SDK	*Software Development Kit* (Kit para Desenvolvimento de Software)
Serpro	Serviço Federal de Processamento de Dados
SHA-1	*Secure Hash Algorithm 1* (algoritmo de resumo seguro 1)

SMTP	*Simple Mail Transfer Protocol* (protocolo simples de transferência de mensagens)
spam	Termo utilizado para mensagens indesejadas
SPAM	Marca registrada da Hormel Foods Corporation
SPB	Sistema de Pagamentos Brasileiro
SPF	*Sender Policy Framework* (infra-estrutura de política de envio)
SRF	Secretaria da Receita Federal
SSH	*Secure Shell* (interface de comandos segura)
SSL	*Secure Sockets Layer* (camada de conexão segura)
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TCP	*Transmission Control Protocol* (protocolo de controle de transmissão)
TI	*Tecnologia da Informação*
Triple DES	*Triple Data Encryption Standard* (padrão de cifragem tripla de dados)
TRT	Tribunal Regional do Trabalho
TST	Tribunal Superior do Trabalho
URL	*Uniform Resource Locator* (localizador uniforme de recursos)

SUMÁRIO

1. Introdução

Este capítulo inicia-se com uma seção que apresenta a importância das mensagens de correio eletrônico (e-mail) para as pessoas e para as organizações. A seção seguinte apresenta um breve histórico das mensagens não autorizadas (*spams*) e os tipos mais comuns destas mensagens. Segue-se mostrando os problemas causados pelo *spam*. Depois é apresentada a pesquisa proposta, seus objetivos, hipóteses e os possíveis referenciais teóricos. O capítulo é finalizado com uma seção justificando a pesquisa, mostrando sua relevância para a comunidade científica e para a sociedade, e outra seção apresentando o restante do trabalho.

1.1. A importância dos e-mails

As mensagens de correio eletrônico, conhecidas como e-mail, representam hoje uma forma de comunicação muito utilizada pela sociedade da chamada Era Digital. A popularização da Internet contribuiu bastante para o aumento da utilização do e-mail, transformando-o num meio de comunicação de massa. Os e-mails são bem mais rápidos que as cartas, mais baratos que as ligações telefônicas e ainda podem ser lidos e respondidos pelo receptor no momento que lhe for mais conveniente.

Para fins pessoais, o e-mail é uma importante forma de comunicação. Para as empresas ele tem se transformado numa excelente ferramenta de trabalho, pois permite a formalização de contatos telefônicos, o envio de propostas e fechamento de negócios, é utilizado para compartilhar planos, fazer notificações, enviar detalhes de projetos, etc.

O uso dos e-mails vem crescendo significativamente desde a popularização da Internet na década de 90. Como pode ser visto na Figura 1, o uso do e-mail como forma de acesso ao serviço de Help Desk da Oxford University cresceu de menos de 2000 mensagens ano fiscal de 1993/4 (julho de 1993 a junho de 1994) para mais de 7000 mensagens em 1996/7. No mesmo período a quantidade de chamadas feitas por telefone ou pessoalmente praticamente permaneceu a mesma. O e-mail criou um novo canal de comunicação e se popularizou rapidamente.

O uso do e-mail na Oxford University continuou crescendo, não só para o acesso ao Help Desk, mas para todos os fins, como pode ser visto na Figura 2. No ano fiscal de 2002/3 já havia uma média de aproximadamente 400 mil mensagens por dia, com um tráfego de aproximadamente 8GB. Nos anos seguintes a quantidade de mensagens cresceu pouco chegando a 500 mil mensagens por dia em 2005/6. Mas, o volume de tráfego cresceu para 15GB por dia. Estas figuras refletem a popularização do e-mail desde os primórdios da década de 90 até os dias de hoje.

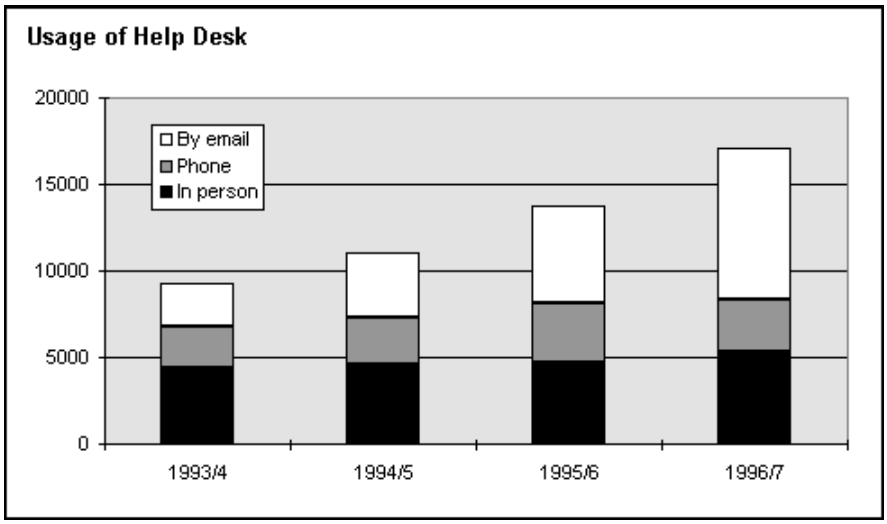

Figura 1 - Uso do Help Desk da Oxford University de 1993 a 1997.
Fonte: www.oucs.ox.ac.uk/internal/annrep/annrep967/help-call-type.gif

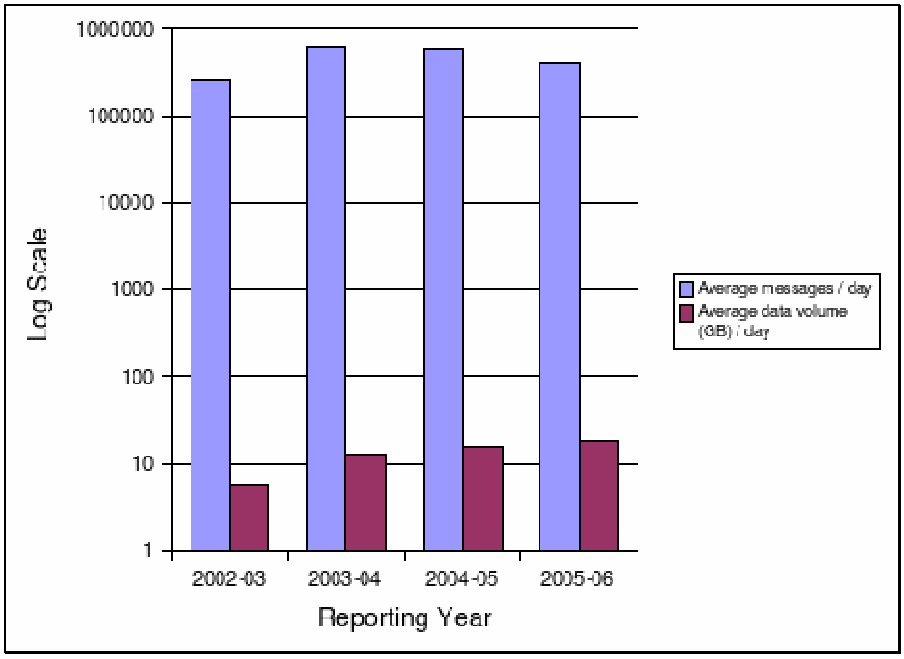

Figura 2 - Média de e-mails e volume por dia da Oxford University de 2002 a 2006.
Fonte: www.oucs.ox.ac.uk/internal/annrep/annrep0506/index.xml.ID=service

1.2. O spam

Por outro lado, a popularização do e-mail também propiciou o envio de mensagens, notícias e propagandas não autorizadas. Esta prática, conhecida como *spam*, tem se tornado uma verdadeira "praga" para os provedores de serviço de Internet, para os administradores de sistemas e de serviços de e-mail. Além do envio direto de *spam* o envio indireto também pode ser conseguido com a exploração de algumas vulnerabilidades presentes nas ferramentas que foram criadas para proporcionar o uso dos e-mails.

A versão mais aceita para o termo "*spam*" tem como base o racionamento de comida que ocorreu na Inglaterra durante e após a Segunda Guerra Mundial. Um dos poucos produtos que não entraram no racionamento era uma marca de presunto suíno chamado "SPAM". A Figura 3 mostra uma fotografia desse presunto. Como as pessoas não tinham muitas opções, comeram bastante esse presunto, enjoaram-se e começaram a rejeitar o produto no pós-guerra. Posteriormente, o grupo de humoristas ingleses Monty Python, usou a palavra "*spam*" num programa humorístico e em filmes ironizando o racionamento de comida durante e após a guerra. A palavra "*spam*" começou então a ser utilizada como sinônimo de algo indesejado e foi também atribuída aos e-mails indesejados [VERISSIMO03].

Figura 3 - Latas de presunto suíno da marca SPAM.

A prática do envio de mensagens indesejadas é conhecida como *spamming*, as mensagens indesejadas são os *spams*, as pessoas que as enviam são conhecidos como *spammers* e as pessoas que buscam evitar a presença destas mensagens nos servidores são conhecidas como *anti-spammers*.

Como o envio de milhões de mensagens de e-mail tem um custo bem mais baixo que o telefone, fax ou correio tradicional, os *spammers* tiram proveito disto e da automação do

envio de mensagens. Mesmo que menos de 0,01% dos destinatários faça o que é esperado pelo *spammer*, seus objetivos podem ser atingidos assim mesmo.

Os tipos mais comuns dos *spams* são mostrados a seguir. O texto foi produzido com base na RFC 2635 [HAMBRIDGE99], na página www.antispam.br/tipos/ do Comitê Gestor da Internet (CGI) no Brasil e na monografia "Segurança em Servidores de Correio Eletrônico" [MARCEL06].

1.2.1. Propagandas

São mensagens oferecendo produtos, serviços, currículo de pessoas, propaganda política, etc. É o tipo mais antigo e mais comum de *spam*. Muitas propagandas são lícitas, mas mesmo assim indesejadas. Por outro lado, boa parte dos produtos ou serviços oferecidos são ilícitos, ilegais ou até mesmo roubados, por exemplo: medicamentos, softwares piratas, diplomas, apostas, cassinos, etc. Logo, nesse caso, os *spammers* procuram esconder bem suas identidades.

1.2.2. Correntes (*chain letters*)

São mensagens enviadas para as pessoas prometendo sorte ou algum tipo de benefício para as pessoas que repassarem a uma quantidade determinada de pessoas num tempo determinado. Paradoxalmente prometem infortúnios ou outros malefícios para as pessoas que interromperem a corrente. A idéia é atingir um número imenso de pessoas num espaço ínfimo de tempo.

1.2.3. Boatos (*hoaxes*)

São mensagens falsas, escritas e enviadas com o propósito de iludir ou mesmo alarmar pessoas. Normalmente, estas mensagens tentam sensibilizar as pessoas alegando que alguém precisa urgentemente de ajuda ou relatando alguma ameaça ou perigo iminente. O real propósito disto é fazer com que o receptor divulgue rapidamente a mensagem para mais pessoas.

1.2.4. Golpes (*scam*)

São mensagens oferecendo produtos ou oportunidades falsas, cujo único propósito é gerar vantagens para o *spammer*. As ofertas mais comuns são de oportunidades de trabalho ou de negócios (normalmente pirâmides) miraculosas, empréstimos (sem fiador), trabalho em casa, etc. A FTC (*Federal Trade Commission*) americana preparou, em 1998, uma lista dos 12 golpes mais comuns, disponível em www.ftc.gov/bcp/conline/pubs/alerts/doznalrt.shtm [FTC98], são eles: oportunidades de negócio, listas e ferramentas de envio de e-mails (*bulk e-mail*), cartas correntes (envolvendo dinheiro), trabalho em casa, fraudes com saúde ou dieta, lucro fácil, mercadorias de graça, oportunidades de investimento, kit decifrador de tv a cabo, garantia de empréstimo ou crédito fácil, recuperação de crédito e promoções de férias a preços incríveis. No Brasil, a página de tipos de fraudes de *spams* do Comitê Gestor da Internet, www.antispam.br/tipos/fraudes/, descreve muito bem cada uma destas fraudes.

1.2.5. Pescaria (*phishing*)

São mensagens que visam iludir o destinatário e obter dados pessoais do mesmo. A primeira forma desses *spams* foi o envio de links para páginas falsas, elas se parecem com páginas reais (de bancos ou sites de compras, por exemplo), o destinatário da mensagem fornece seus dados e depois é repassado para a página real. Nesse caso, o principal objetivo é obter credenciais de acesso (usuário e senhas), para depois o *spammer* fazer desvios, transferências ou compras pela Internet.

Posteriormente, os *phishing spammers* passaram a enviar mensagens disfarçadas de *spam* comercial, mensagens comuns nas organizações ou mensagens pessoais de pessoas comuns (para ser associadas a pessoas conhecidas), solicitando alguns dados do destinatário para completar um determinado cadastro. São oferecidos formulários no próprio e-mail ou em páginas específicas para que o destinatário possa “completar” seus dados.

O termo *phishing* (de *fishing*, pescar em inglês) é utilizado pelos *spammers*, pois o e-mail é a “isca” utilizada para “pescar” dados confidenciais dos destinatários. Como novos tipos de *phishing* podem surgir a qualquer momento é importante estar atento e notificar as autoridades para as novas modalidades desta fraude.

1.2.6. Ameaças, brincadeiras, difamação e ofensivos

São *spams* contendo difamação de pessoas (ex-amigos, ex-cônjuges, ex-namorados, etc.) ou empresas, brincadeiras inconvenientes ou mesmo ameaças. O receptor sentindo-se lesado de alguma forma pode procurar a polícia para tratar as ameaças e para as difamações processar o *spammer* por calúnia e difamação. Os *spams* ofensivos divulgam materiais racistas, violentos, agressivos, faz apologia à violência, divulgam ideologias extremistas contra minorias, divulgam pedofilia ou xenofobia (aversão ao que é diferente). Logicamente, em todos os casos, os *spammers* tentam "proteger" suas identidades.

1.2.6. Programas maliciosos (vírus, vermes e cavalos de tróia)

São mensagens que carregam consigo códigos maliciosos ou possuem *links* para locais onde esses códigos podem ser instalados. Para iludir o destinatário, os *spammers* usam as mesmas técnicas do *phishing*. Os códigos maliciosos mais comuns, enviados através desse tipo de mensagem, são os vírus, os vermes (*worms*) e cavalos de tróia (*trojans horse*).

Os vírus, normalmente, são instalados em arquivos executáveis no sistema do destinatário. Uma vez instalado, os vírus procuram meios de se propagarem para outros computadores. As ações maléficas dos vírus incluem perturbar o usuário, apagar arquivos, danificar a configuração do sistema, etc. Os vermes, por outro lado, não precisam de arquivos para se propagar e têm ações maléficas menores na máquina do usuário. Os cavalos de tróia, uma vez instalados, abrem portas ou concedem privilégios a outro programa, rodando em máquinas controladas pelo *spammer*, permitindo cópias, alterações ou exclusões de arquivos, dados ou registros do sistema. Os cavalos de tróia também são utilizados para fazer da máquina do destinatário uma máquina controlada pelo *spammer*, que a utiliza para enviar *spams* ou contaminar outros computadores.

Na página www.antispam.br/tipos/fraudes/, do Comitê Gestor da Internet no Brasil, existe uma boa descrição desse tipo de *spam*, as mensagens mais comuns, como identificá-las e recomendações de ações.

1.3. Os problemas causados pelo spam

A Figura 4 mostra que mais de 56% das mensagens interceptadas pela MessageLabs [MSGLABS06] (fornecedor de interceptadores de *spam*) de abril de 2006 a abril de 2007, em seus *data centers* em todos os continentes, eram *spams*.

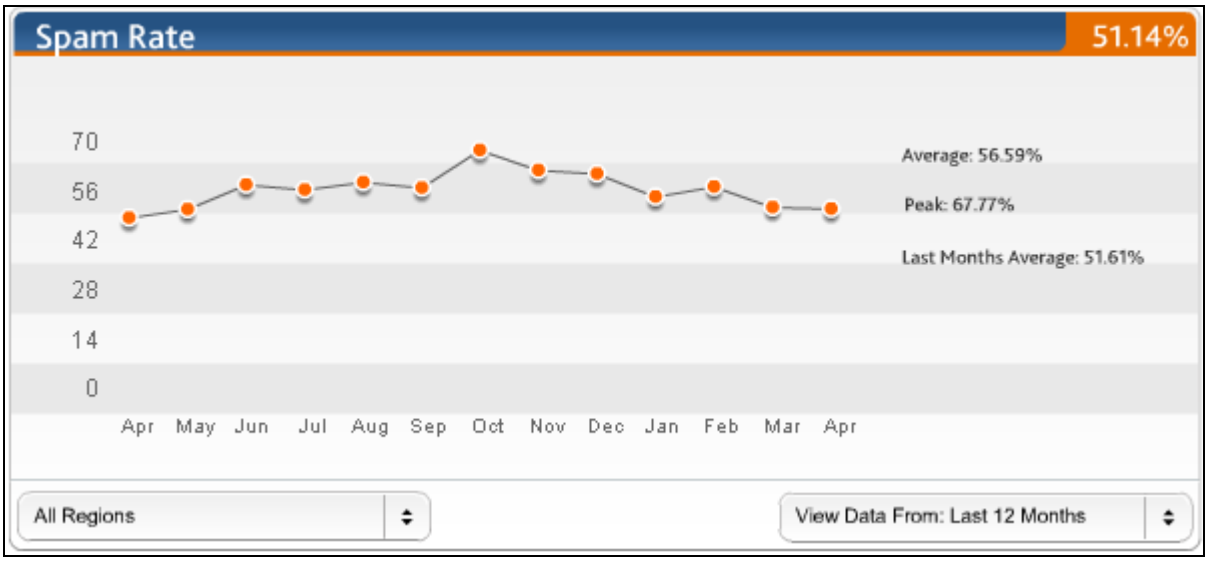

Figura 4 - Percentual de *spams* nos e-mails de abril/6 a abril/7 (Fonte: MessageLabs).

Segundo o Comitê Gestor da Internet no Brasil [ANTISPAM06], os *spams* provocam os seguintes problemas:

- Não recebimento de e-mails: A maioria dos provedores limita o tamanho das caixas postais. Os *spams* podem lotar as caixas postais, causando o retorno de mensagens desejadas.
- Gasto desnecessário de tempo: O usuário gasta tempo identificando, filtrando e eliminando *spams*.
- Aumento de custos: Os usuários e as empresas acabam pagando a conta do envio dos e-mails, direta (tempo de conexão) ou indiretamente (tempo desnecessário).
- Perda de produtividade: As pessoas que utilizam e-mails como ferramentas de trabalho gastam indevidamente tempo com os *spams* (10% do tempo segundo pesquisa da MessageLabs [MODULO02]).
- Conteúdo impróprio ou ofensivo: Como não há controle do conteúdo dos *spams*, os usuários podem julgá-los impróprios ou ofensivos.

- Prejuízos financeiros causados por fraude: Os *spams* de fraudes, golpes e pescaria causam prejuízos financeiros aos destinatários e às instituições que têm seus nomes envolvidos direta ou indiretamente com esses *spams*.

1.4. Sobre esta pesquisa

O tema desta pesquisa é o envio e a recepção de correios eletrônicos (e-mails). O problema a ser abordado é a transmissão segura de e-mails para minimizar os *spams*. No contexto desta pesquisa, são considerados e-mails seguros aqueles que apresentam confidencialidade (quando necessária), autenticidade e integridade entre o emissor e o receptor. No contexto deste trabalho:

- Confidencialidade: significa que a mensagem só está legível para o emissor e o receptor. Caso ela seja interceptada por um espião, não será legível para ele. Isto é garantido por criptografia da mensagem.
- Autenticidade: significa que a mensagem é autêntica, ou seja, a origem e a identidade do emissor estão vinculadas e são autênticas. Esse vínculo garante também o não repúdio, ou seja, o emissor não pode repudiar a emissão da mensagem. Isto é garantido pelo uso da assinatura digital do emissor.
- Integridade: significa que a mensagem não foi alterada desde o emissor até o receptor. A assinatura digital também garante isto.

Segundo Wagner Gomes, citando Henrique Faulhaber (conselheiro do Comitê Gestor de Internet do Brasil), atualmente os *spams* (mensagens eletrônicas não solicitadas, enviadas em massa para vários destinatários) representam quase 90% dos e-mails enviados cotidianamente [GOMES06].

Quanto ao uso do e-mail como forma de prova documental, de acordo com Leitão Jr. [LEITÃOJR02] há duas correntes no Brasil. Uma que adota a admissibilidade direta e indireta e outra que se pauta pela admissibilidade direta e condicionada. Em que pese às distinções entre as duas correntes. Para ambas (assim como para qualquer tipo de documento) a suspeita quanto à sua autenticidade transfere o ônus da prova para o autor. Logo, e-mails sem assinatura digital são facilmente “derrubados” como prova ou têm a sua importância reduzida apenas a indícios. Isso se deve à dificuldade de se provar a autenticidade de um e-mail, o que requer uma perícia tanto na origem quanto no destino da mensagem, comprovando que essa partiu realmente na origem, não sofreu alterações no

caminho e foi recebida com integridade no destino. Como um e-mail não assinado digitalmente pode ser interceptado e alterado desde a origem até mesmo no próprio destino e em qualquer equipamento que estiver no meio desse caminho, utilizá-lo como prova é praticamente inviável.

Diante do exposto cabe a seguinte proposição de problema: É viável e possível reduzir significativamente o envio de *spams*, utilizar os e-mails de forma confidencial e comprobatória documentalmente?

1.5. Hipóteses

Este trabalho considera a estratégia mostrada na Figura 5 e descrita a seguir:

- E-mails seguros (confidencialidade, autenticidade e integridade) podem ser utilizados como provas formais.
- Se os e-mails seguros puderem ser utilizados como prova formal é possível atribuir responsabilidade aos emissores.
- Se os emissores de *spam* puderem ser responsabilizados por seus atos, eles diminuirão a emissão desse tipo de mensagem.
- Se o uso de e-mails seguros for simples sua adoção será inevitável, pois a necessidade e a infra-estrutura para esse tipo de e-mails já existem.

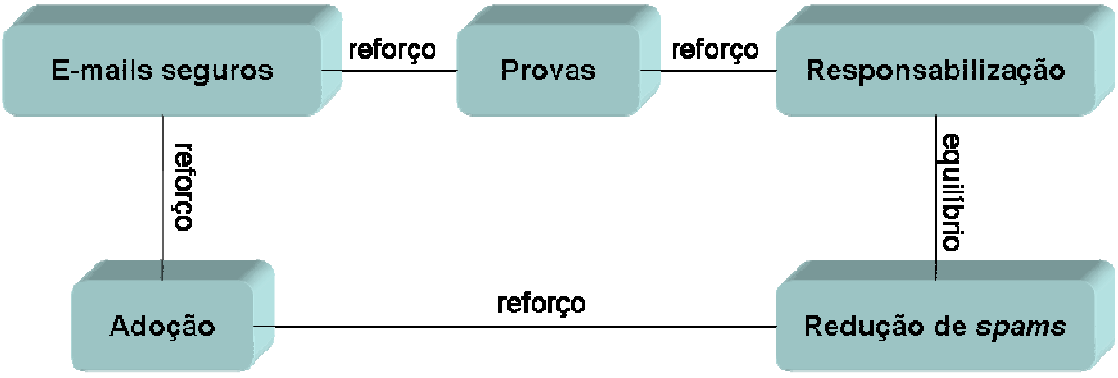

Figura 5 - Estratégia de uso dos e-mails seguros para redução dos *spams*.

Desta estratégia deriva-se o seguinte conjunto de hipóteses a serem investigadas:

- Deve existir um protocolo que permita o uso de e-mails seguros.

- Se não existir o referido protocolo, um novo protocolo deverá ser criado de forma que possa ser encapsulado nos protocolos existentes (POP3, SMTP e S/MIME).
- E-mails seguros podem ser utilizados como provas documentais.
- A adoção dos e-mails seguros reduz significativamente os *spams*, pois os e-mails cuja origem não possa ser comprovada não serão mais aceitos. Se existir *spams* nos e-mails aceitos, a origem poderá ser comprovada e o emissor responsabilizado por isto, o que também provocará redução desse tipo de mensagem.

Se já existir um protocolo que permita o uso de e-mails seguros, a adoção pela comunidade será mais fácil que de um protocolo novo. Por outro lado, um novo protocolo encapsulado dentro dos existentes atualmente torna sua adoção transparente. O não repúdio da origem e a vinculação desta a uma identidade, tornam o emissor de *spam* passível de ser responsabilizado civil e criminalmente por seus atos. Portanto, confirmando-se estas hipóteses, é possível reduzir o envio de *spams* e os prejuízos que eles geram.

1.6. Objetivos

Este trabalho tem os seguintes objetivos:

- Verificar se existe um protocolo que permita o envio e a recepção de e-mails seguros. Caso esse protocolo não exista, propor um.
- Verificar se o protocolo identificado no objetivo anterior pode ser encapsulado nos protocolos existentes atualmente (POP3, SMTP e S/MIME) de forma a tornar transparente a sua adoção.
- Se necessário, implementar o protocolo proposto.
- Criar um ambiente de teste (contendo no mínimo dois clientes e um servidor de e-mails) e experimentar a utilização do protocolo.
- Divulgar os resultados deste trabalho de forma que a comunidade científica e técnica possam ter acesso a seus resultados.

1.7. Justificativa

A resolução do problema proposto é um ótimo desafio científico e representa a geração dos seguintes benefícios para a sociedade:

- Facilidade operacional e comprobatória para as empresas que pretendem utilizar o e-mail como prova.
- Garantia de confidencialidade, autenticidade e integridade das mensagens trocadas por e-mails.
- Redução dos *spams* gerando os benefícios marginais a seguir:
    - Reduz a perda de e-mails solicitados.
    - Reduz o gasto desnecessário de tempo.
    - Reduz custos.
    - Aumenta a produtividade.
    - Diminui as fraudes eletrônicas.

1.8. Referencial teórico

No desenvolvimento deste trabalho será preciso investigar trabalhos científicos já produzidos a respeito do tema, especialmente o artigo do SANS (SysAdmin, Audit, Network, Security) intitulado "*Securing E-Mail*" escrito por Sharipah Setapa em 2001 [SETAPA01], o qual descreve o tema de forma abrangente e resume parte do conhecimento existente sobre o assunto.

Para validar ou refutar algumas hipóteses de pesquisa será preciso estudar outro artigo do SANS denominado "*Utilizing Open-Source Software to Build a (Relatively) Secure, Spam- and Virus-Free Mail Service*", escrito em 2004 por David Bailey [BAILEY04]. Também será preciso estudar um artigo preparado pelo pessoal do MIT (Massachusetts Institute of Technology) e da Amazon chamado "*How to Make Secure E-mail Easier To Use*", escrito em 2005 por Garfinkel, Margrave, Schiller e outros [GARFINKEL05].

Também será preciso analisar soluções de transmissão de e-mails seguros, tais como: *Sun Secure Mail* (www.sun.com/solutions/documents/solution-sheets/te_sunsecure_mail.pdf), *Secure E-mail User Guide - Outlook 2000* (https://www.wellsfargo.com/com/cps/), Crypto Mail (www.cryptomail.org/), PGP (Pretty Good Privacy), etc.

Os conceitos teóricos desse trabalho, especialmente conhecimentos de criptografia e assinaturas digitais, foram descritos de forma muito clara, precisa e objetiva por William Stallings em seu livro "*Cryptography and Network Security: Principles and Practice*" de 1999 [STALLINGS99].

1.9. Organização do trabalho

No capítulo 2 é apresentado um resumo da criptografia de chave pública e o funcionamento dos sistemas de e-mails com os agentes envolvidos nesses sistemas. No capítulo 3, utilizando o laboratório montado para a pesquisa, é investigado se os principais protocolos existentes atualmente podem ser considerados seguros, onde se conclui que o S/MIME é um protocolo seguro. No capítulo 4 é descrito como se utilizar o protocolo S/MIME para enviar e receber mensagens cifradas e assinadas digitalmente. O capítulo 5 foi dedicado à análise do uso de e-mails como provas em questões jurídicas. Finalmente, no capítulo 6 são apresentadas as conclusões e os possíveis trabalhos futuros.

2. Criptografia de chave pública e funcionamento do e-mail

A primeira seção deste capítulo apresenta um resumo da criptografia de chave pública aplicada à transmissão de mensagens. O propósito desta seção é subsidiar o entendimento do que é considerado um e-mail seguro nesse trabalho, ela não visa esgotar os assuntos de criptografia de chave pública, assinatura e certificado digital.

Na segunda seção do capítulo é apresentada a estrutura de um sistema de e-mail apresentando os agentes envolvidos e ressaltando a importância dos protocolos nesse serviço.

2.1. Criptografia de chave pública

A criptografia teve seu início na Grécia antiga. O objetivo fundamental da criptografia é transformar um texto legível, chamado de texto plano, em um texto codificado, chamado de texto cifrado. Cifrar é transformar o texto plano no texto cifrado. Decifrar é transformar o texto cifrado no texto plano original. Para cifrar e decifrar são utilizados algoritmos e chaves. Os algoritmos são métodos de transformação de um texto em outro, os algoritmos utilizam chaves para cifrar e decifrar [STALLINGS99]. Por exemplo, seja o algoritmo “texto + chave”, usando a chave 3, cifra-se o valor 4 obtendo 7 (4 + 3) e decifra-se o 7 obtendo o valor 4 (7 - 3). A Figura 6 mostra resumidamente estes processos.

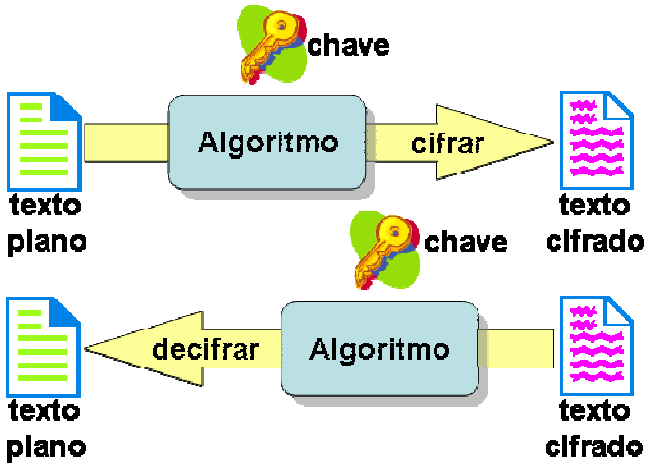

Figura 6 - Processo simétrico de cifrar e decifrar.

Nos processos de cifrar e decifrar podem ser utilizadas a mesma chave em ambos os processos, essa é a criptografia simétrica, ou chaves diferentes para cada processo, nesse caso tem-se a criptografia assimétrica ou criptografia de chave pública, que usa uma chave pública e outra privada. Na criptografia simétrica, a mesma chave deve ser compartilhada tanto por quem cifra quanto por quem decifra a mensagem, esse processo é conhecido como troca de chaves. Esta troca de chaves deve ser feita de forma segura, pois todos os que tiverem a chave podem decifrar a mensagem [STALLINGS99].

Na criptografia de chave pública são utilizadas duas chaves, uma privada (conhecida somente pelo seu proprietário) e uma pública que pode ser de conhecimento público. Existe uma relação entre estas duas chaves, gera-se a chave pública a partir da chave privada. Mas, tendo-se a chave pública é praticamente impossível obter-se a chave privada [STALLINGS99]. A empresa americana RSA mantém um desafio de obtenção da chave privada a partir da chave pública, pagando recompensas de 10 a 200 mil dólares para quem conseguir quebrar as chaves. As chaves de até 640 bits já foram quebradas. As chaves de 704 a 2048 bits, até o momento da escrita deste texto, ainda não haviam sido quebradas. O desafio pode ser visto na página www.rsa.com/rsalabs/node.asp?id=2093. Logo, a chave privada deve ser mantida de forma segura pelo proprietário da mesma.

2.1.1. Confidencialidade

Para garantir a confidencialidade de uma mensagem, ela deve ser cifrada com a chave pública do destinatário. Ao receber a mensagem o destinatário a decifra utilizando sua chave privada [STALLINGS99]. A Figura 7 mostra o processo de envio e recepção de uma mensagem cifrada para um usuário chamado João, utilizando criptografia de chave pública. A cifragem é feita no emissor utilizando a chave pública do João. A decifragem é feita pelo João utilizando a chave privada dele.

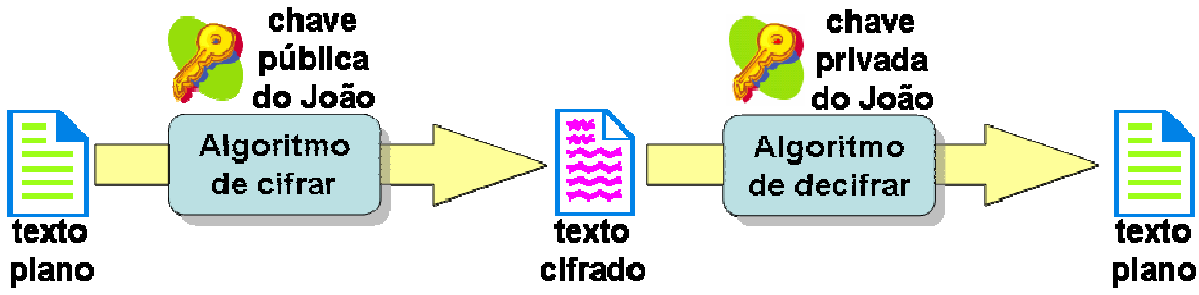

Figura 7 - Envio e recepção de mensagens cifradas com chaves públicas.

2.1.2. Autenticidade

Para garantir a autenticidade de uma mensagem, utiliza-se um processo semelhante ao confidencialidade, invertendo-se o uso das chaves. A mensagem é cifrada com a chave privada do emissor e decifrada com a chave pública dele. Assim, somente o emissor pode ter gerado a mensagem, já que somente ele possui sua chave privada [STALLINGS99]. A Figura 8 mostra o envio de uma mensagem autenticada de uma usuária chamada Maria para um usuário chamado João. A mensagem é cifrada na máquina da Maria utilizando a chave privada dela e decifrada na máquina do João utilizando a chave pública da Maria.

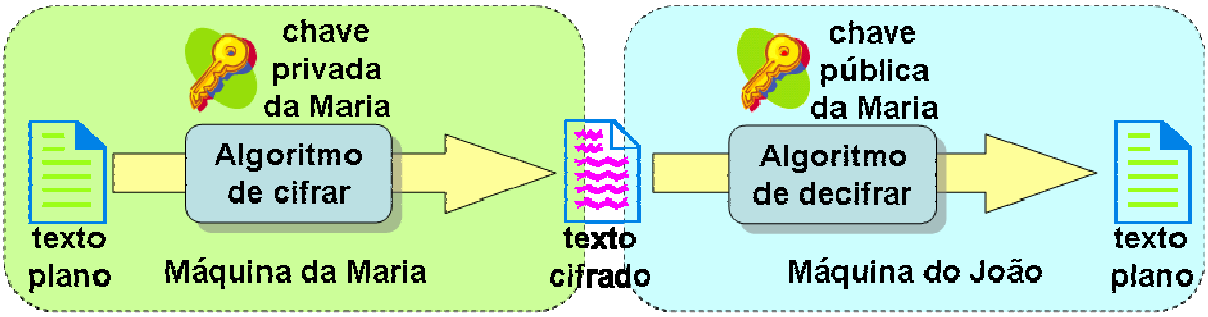

Figura 8 - Garantindo autenticidade de mensagens.

2.1.3. Assinatura Digital

A assinatura digital utiliza o conceito de autenticidade com chave pública, apresentado na seção anterior, acrescentando o uso de uma função *hash*. A função *hash* lê um texto qualquer e gera um número correspondente ao texto. Esse número tem duas propriedades: ele tem tamanho constante independentemente do tamanho do texto de origem e é uma espécie de identidade do texto, ou seja, uma mudança no texto (por menor que seja) gera uma modificação no resultado da função *hash*. A assinatura digital consiste em usar uma função *hash* no texto plano, cifrar o resultado com a chave privada do emissor e agregar esta informação à mensagem. Para checar a assinatura o receptor deverá aplicar a função *hash* ao texto e comparar o resultado com o obtido ao decifrar a assinatura enviada utilizando a chave pública do emissor [STALLINGS99].

A Figura 9 mostra o processo de assinatura digital aplicado a uma mensagem emitida por uma usuária chamada Maria para um usuário chamado João. O texto plano da mensagem original é passado na função *hash*. O valor *hash* é então cifrado com a chave privada da Maria gerando a assinatura digital. Finalmente, a assinatura digital é anexada ao texto plano original formando o corpo da mensagem a ser enviada ao João. Como os algoritmos de

cifrar usando chaves públicas são complexos e lentos, a função *hash* melhora o desempenho do processo, pois o algoritmo de cifrar é aplicado somente ao valor *hash* do texto plano original. Como o valor *hash* tem tamanho pré-determinado, esse processo terá um tempo baixo e homogêneo.

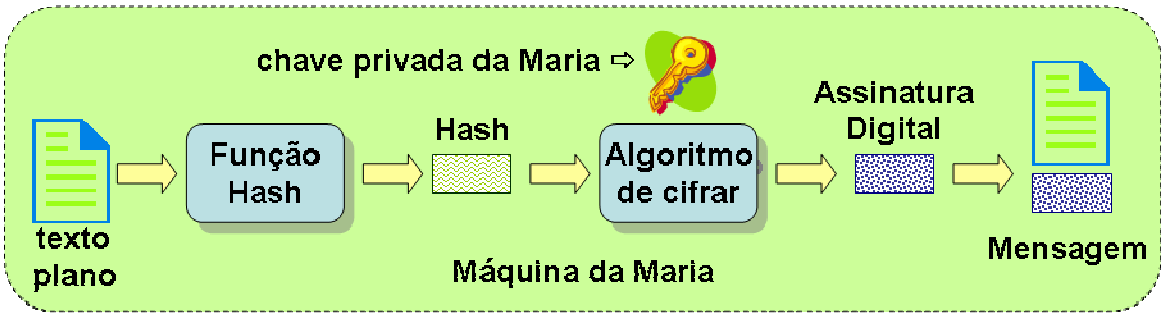

Figura 9 - Assinando digitalmente mensagens.

A Figura 10 mostra o processo de comprovação da veracidade da assinatura digital. O receptor (João) da mensagem deve: calcular o valor *hash* do texto plano original (sem a assinatura) e decifrar a assinatura digital utilizando a chave pública do emissor (Maria). Se os valores resultantes forem iguais, conclui-se que a assinatura está comprovada e o documento está íntegro.

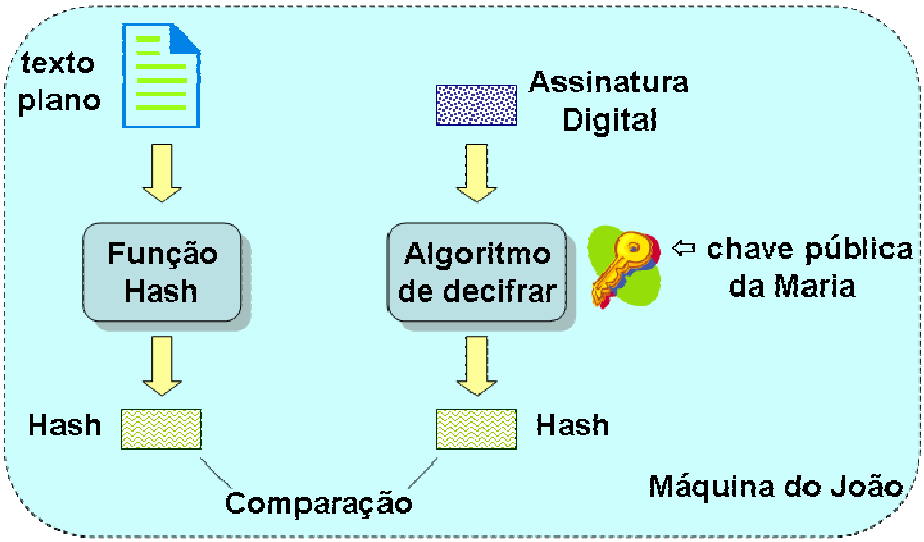

Figura 10 - Comprovando a assinatura digital.

2.1.4. Certificação Digital

Nesse trabalho foi considerado um e-mail seguro aquele que apresenta: confidencialidade, autenticidade e integridade. Como foi visto nas seções anteriores, a assinatura digital garante autenticidade e integridade. Se for desejado a confidencialidade, basta que o texto

plano do e-mail seja cifrado com a chave pública do destinatário. A Certificação Digital é a tecnologia que proporciona os mecanismos de segurança necessários para os e-mails seguros.

O Certificado Digital é um documento eletrônico que contém informações do proprietário do certificado. Dentre as informações do certificado, tem-se a identificação (nome), a chave pública do proprietário, período de validade, número de série, nome e assinatura digital da entidade que emitiu o certificado. A chave pública será utilizada nos processos de confidencialidade e verificação da assinatura digital. O Certificado Digital pode ser emitido e reconhecido por uma Autoridade Certificadora (CA), que nesse caso funciona como se fosse um cartório de registro e reconhecimento de firmas (assinaturas). O período de validade do certificado restringe o período que ele pode ser utilizado para assinar documentos, embora o reconhecimento da assinatura possa ser feito mesmo após o término do período de validade do certificado [ITI05].

Segundo o ITI (Instituto Nacional de Tecnologia da Informação, www.iti.gov.br) em Junho de 2007 mais 600 mil brasileiros possuíam certificados digitais. O ITI prevê que no final desse ano serão mais de um milhão de brasileiros com certificados [JANUARIO07]. Os certificados digitais foram reconhecidos pelo governo brasileiro em dezembro de 2006, na Lei 11419, que permite aos advogados assinarem petições, iniciar um processo, etc. utilizando um certificado digital como forma de assinatura. Da mesma forma, diários da justiça podem ser publicados e assinados digitalmente e entram em vigor, mesmo antes do diário ser impresso em papel.

No Brasil, as Autoridades Certificadoras para serem credenciadas devem ser reconhecidas pela ICP-Brasil (Infra-Estrutura de Chaves Públicas Brasileira, www.icpbrasil.gov.br, instituída pela MP 2200/2001). As CA já credenciadas são: e-CAC (Centro Virtual de Atendimento ao Contribuinte da Secretaria da Receita Federal), Serpro (Serviço Federal de Processamento de Dados), CertiSign, Serasa, IMESP (Imprensa Oficial do Estado de São Paulo), PRODEMG (Empresa de Processamento do Governo de Minas Gerais) e CEF (Caixa Econômica Federal). O ICP-Brasil é a Autoridade Certificadora Raiz, ou seja, autoridade que pode certificar outras autoridades a emitir e validar certificados. Os cartórios através da ANOREG (Associação dos Notários e Registradores do Brasil) e os bancos através da FEBRABAN (Federação Brasileira de Bancos) estão se preparando para entrar nesse mercado [FUSCO05]. Diante disto, espera-se a popularização dos certificados digitais nos próximos anos.

2.2. Funcionamento dos sistemas de e-mail

A Figura 11 mostra, de uma forma bem simples, o funcionamento de um e-mail. Existe um emissor, aquele que escreve e envia a mensagem, a Internet (meio utilizado) e o receptor, aquele que recebe a mensagem. Os protocolos são responsáveis pelo envio, transmissão e recepção das mensagens. Um dos princípios do e-mail é que o receptor não precisa estar on-line (conectado na Internet) quando a mensagem é enviada. Como isto é possível?

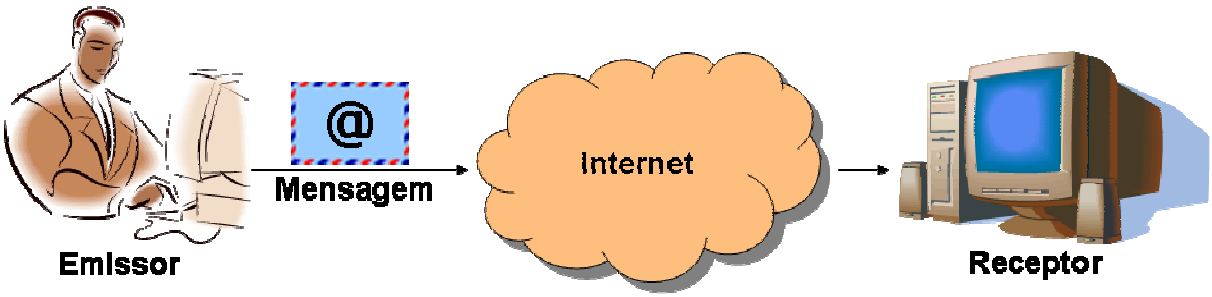

Figura 11 - Funcionamento do e-mail.

Para entender como a mensagem trafega na Internet é necessário identificar alguns elementos responsáveis por isto, os agentes. Dentro dos sistemas das máquinas do emissor e do receptor existem agentes de e-mail do usuário ou MUA (*Mail User Agent*). Na Internet existem dois agentes de transferência de e-mail os MTA (*Mail Transfer Agent*). Um dos MTA fica no servidor onde o emissor tem sua conta de e-mail e o outro no servidor onde o receptor tem sua conta de e-mail. No servidor onde o receptor tem conta de e-mail existe o agente de entrega de e-mail, MDA (*Mail Delivery Agent*), e o agente de acesso ao e-mail o MAA (*Mail Access Agent*) que é responsável pela entrega da mensagem ao MUA do receptor. A Figura 12 detalha esta estrutura.

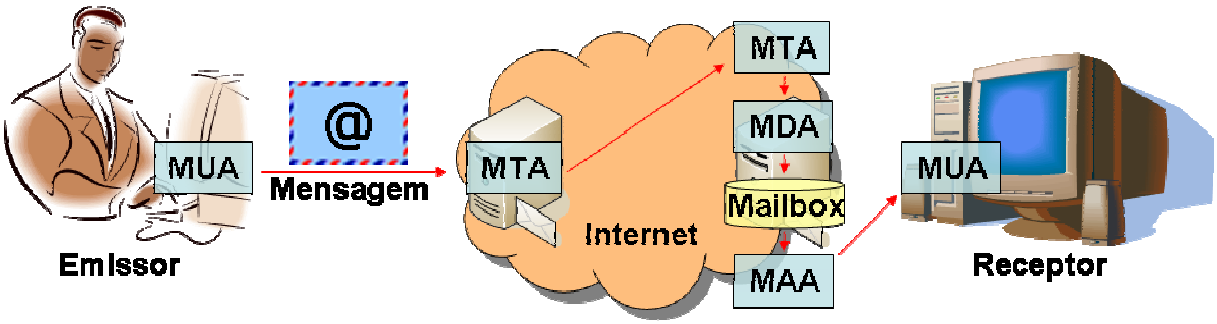

Figura 12 - Os agentes MUA, MTA, MDA e MAA.

A transferência da mensagem ocorre em quatro etapas. Na primeira o MUA do emissor envia a mensagem ao MTA do servidor onde ele tem conta de e-mail. Na segunda, o MTA do servidor onde o emissor tem conta de e-mail envia a mensagem ao MTA do servidor

onde o receptor tem conta. Na terceira o MTA do servidor onde o receptor tem conta envia a mensagem ao MDA. Finalmente, em algum momento, o receptor solicita suas mensagens ao MUA, o MUA busca as mensagens no MAA do servidor onde o receptor tem conta de e-mail. O MAA busca as mensagens no MDA do receptor e entrega ao MUA concluindo a entrega da mensagem.

Assim, mesmo que o receptor não esteja conectado no momento de envio da mensagem pelo emissor, a mensagem pode ser entregue no servidor onde o receptor tem sua conta de e-mail. Quando o receptor se conectar na Internet e no servidor onde ele tem conta, a última transferência é realizada, concretizando a entrega da mensagem.

2.2.1. MUA (*Mail User Agent*)

O MUA é o software que oferece ao usuário a acessibilidade ao seu sistema de e-mail. As principais funções do MUA são conectar-se ao MTA onde o usuário tem sua conta de e-mail, enviar suas mensagens, conectar-se ao MAA onde o usuário tem conta e receber as mensagens dele. A Figura 13 mostra uma tela do Outlook da Microsoft, um dos MUA mais utilizados. Outros MUA comuns são: Lotus Notes, Outlook Express, Mozilla, Netscape, etc.

A transferência das mensagens entre os agentes é feita pelos protocolos. Os mais comuns são o SMTP (*Simple Mail Transfer Protocol*), utilizado para enviar mensagens, e o POP (*Post Office Protocol*), utilizado para receber mensagens. Eventualmente são utilizados os protocolos: IMAP (*Internet Message Access Protocol*) para recepção e arquivamento de mensagens, MIME (*Multipurpose Internet Mail Extensions*) e o S/MIME (*Secure MIME*).

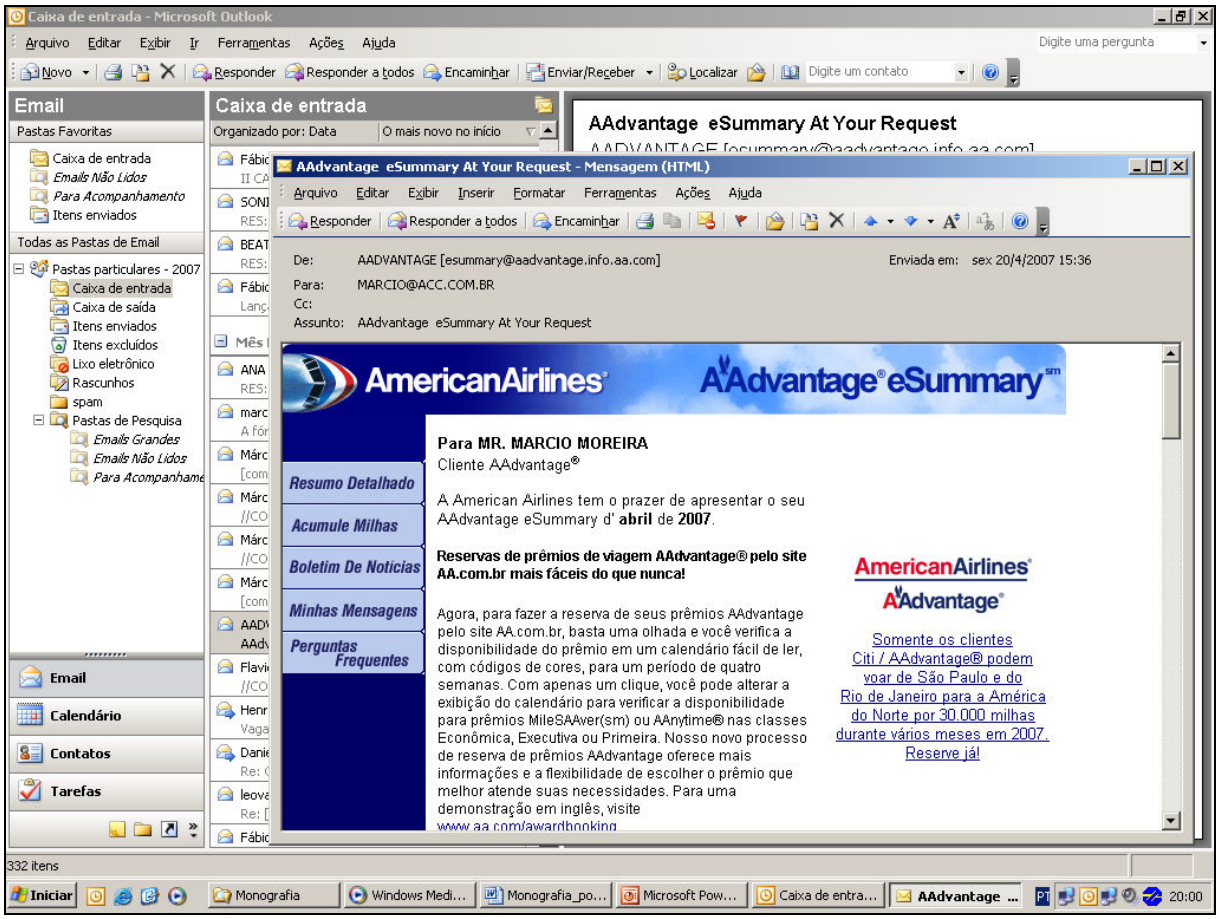

Figura 13 - Exemplo de MUA: Microsoft Outlook.

2.2.2. MTA (*Mail Transfer Agent*)

O MTA é o software que é responsável por receber a mensagem do MUA do emissor e repassá-la para o MTA do receptor. Uma vez no MTA do receptor, esse MTA tem a responsabilidade de repassá-la ao MDA. Em essência, o MTA é um agente de transporte da origem até o servidor que faz a entrega ao receptor (MDA do receptor). O protocolo mais comum destas transferências é o SMTP. Exemplos de MTA: sendmail (mais comum), postfix, gmail, etc. No ambiente Windows, o MTA mais conhecido é o Microsoft Exchange. A Figura 14 mostra os agentes e os protocolos mais utilizados entre eles.

O MTA armazena toda a mensagem em uma pasta temporária e depois a repassa a outro MTA ou MDA (dependendo se a mensagem é para esse servidor local ou outro remoto), ou seja, trabalha no princípio "*store and forward*". A cada transmissão uma linha "*received*" é registrada no cabeçalho da mensagem identificando por onde a mensagem passou. Isto garante a entrega da mensagem.

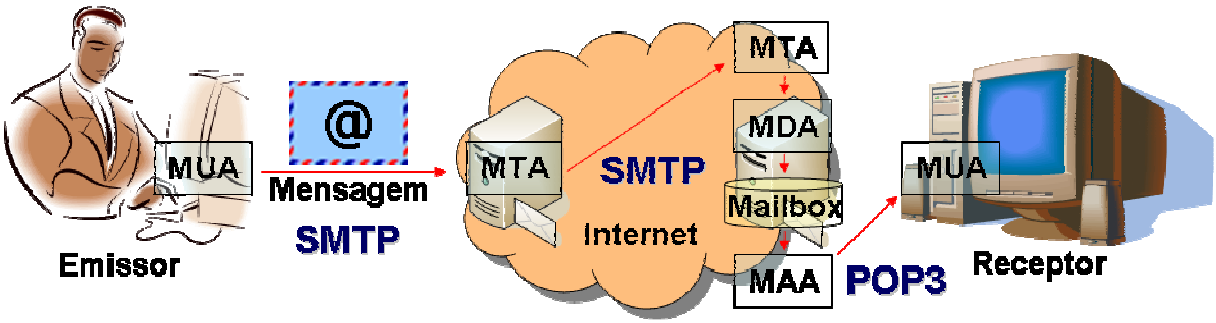

Figura 14 - Os protocolos mais usuais de transporte (SMTP) e entrega (POP3).

2.2.3. MDA (*Mail Delivery Agent*)

O MDA é o software responsável por receber a mensagem do MTA e armazená-la na caixa de correio do receptor. O protocolo mais comum nesta operação é o SMTP. O MDA mais conhecido é o procmail no ambiente Linux e o Microsoft Exchange no ambiente Windows.

2.2.4. MAA (*Mail Access Agent*)

O MAA é o software que permite ao MUA do receptor conectar-se e baixar suas mensagens. O MAA busca as mensagens na caixa postal do receptor e as entrega ao MUA utilizando normalmente o protocolo POP3, eventualmente se utiliza também o IMAP. O papel dos agentes MAA normalmente é exercido pelo mesmo software MDA. Logo, os mais conhecidos são o procmail e o Exchange.

3. Análise dos protocolos existentes

Este capítulo investiga a hipótese de que “deve existir um protocolo que permita o uso de e-mails seguros”. Se esta hipótese for comprovada, será preciso apresentar no capítulo seguinte como utilizar esse protocolo. Do contrário, deve-se verificar a possibilidade de definir um protocolo e encapsulá-lo dentro dos protocolos já existentes.

Para investigar a hipótese proposta, serão investigados os protocolos disponíveis e mais utilizados atualmente. Esta investigação será conduzida considerando os seguintes aspectos de segurança: confidencialidade, autenticidade e integridade. Não se pretende com esse trabalho explicar todos os detalhes dos protocolos, apenas saber se eles podem ser considerados seguros ou não.

Para realização das investigações propostas, como laboratório de testes, será utilizada a estrutura mostrada na Figura 15. Para interceptação de pacotes será utilizado o Ethereal como ferramenta. O Ethereal é um software que intercepta e analisa pacotes de rede, disponível em: www.ethereal.com. As máquinas do Usuário A, B e do espião usam o Windows XP. Para simular a interceptação e o trabalho do espião, a conexão entre o Provedor A e o Usuário A será interceptada utilizando-se um hub.

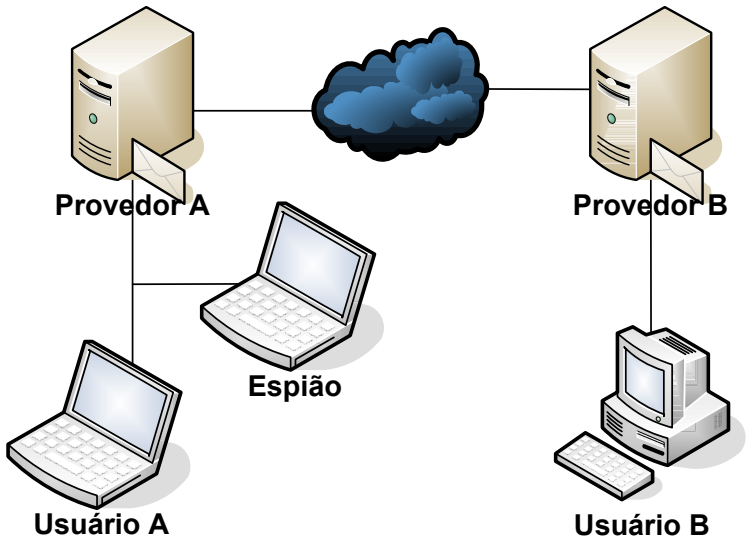

Figura 15 - Estrutura utilizada como laboratório de testes.

3.1. SMTP (Simple Mail Transfer Protocol)

O protocolo SMTP é o padrão de fato no envio de e-mail na Internet. Ele foi definido na RFC 821 [POSTEL82] e complementado no capítulo 5 da pela RFC 1123 [BRADEN89]. O protocolo usado atualmente é uma variação do SMTP conhecido como ESMTP (*Extended* SMTP) definido pela RFC 2821 [KLENSIN01], mas que o mercado ainda continua chamando de SMTP.

Esse protocolo é utilizado para enviar mensagens do MUA do emissor para o MTA do servidor onde ele tem conta. Também é utilizado para enviar mensagens do MTA do emissor para o MTA do receptor. Para simplificar é adotada a seguinte terminologia: “C” (cliente) para a máquina de origem e “S” (servidor) para máquina de destino do protocolo SMTP. O protocolo tem duas fases, uma de autenticação e outra de envio das mensagens. A autenticação pode ser requerida ou não. Como se busca o envio seguro de mensagens deve-se preferir servidores que requeiram autenticação. O protocolo ESMTP prevê o uso de autenticação segura, ou seja, as credenciais (usuário e senha) são enviadas de forma criptografada.

Para testar esta afirmação, foi enviado um e-mail para um servidor que requer autenticação segura e interceptado todos os pacotes SMTP trafegados. O cliente enviou o pacote “AUTH LOGIN”, o servidor respondeu com o código 334 (Ok) em seguida o cliente enviou a credencial para autenticação. Esse pacote está mostrado na Figura 16, note que a credencial foi enviada de forma criptografada.

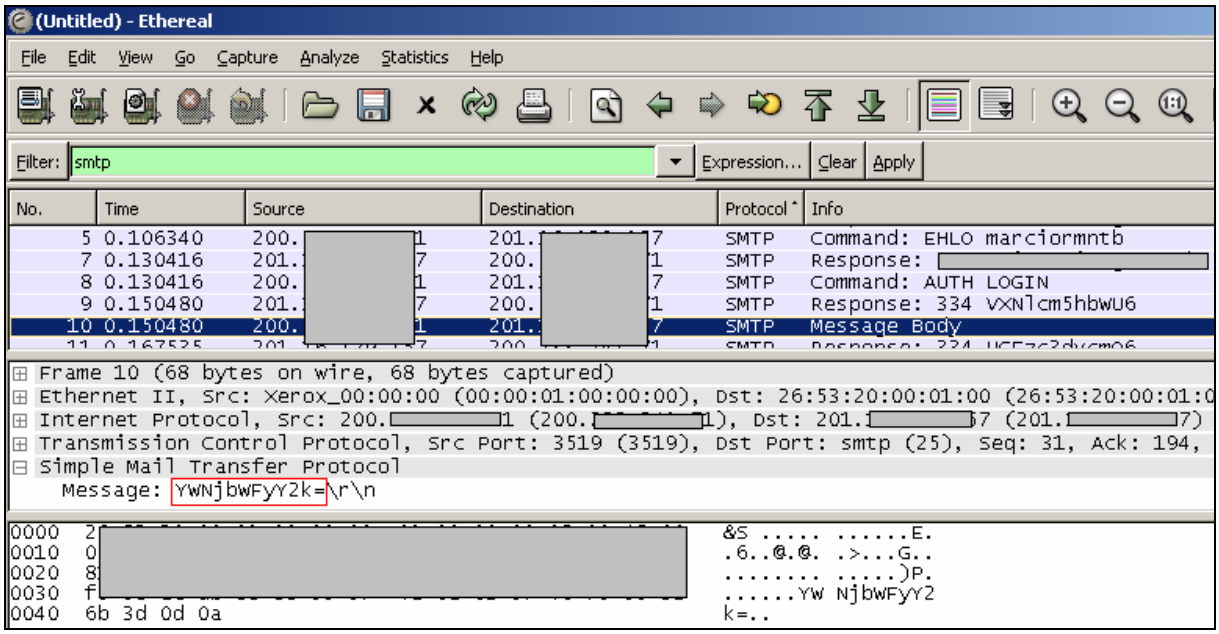

Figura 16 - Envio de credencial segura no SMTP.

Na segunda fase o e-mail é enviado. A RFC 2821 [KLENSIN01] traz um exemplo, mostrado na Figura 17, do diálogo de envio de um e-mail do usuário Smith, da máquina bar.com (cliente), para o usuário Jones na máquina foo.com (servidor).

```
S: 220 foo.com Simple Mail Transfer Service Ready
C: EHLO bar.com
S: 250-foo.com greets bar.com
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
C: MAIL FROM:<Smith@bar.com>
S: 250 OK
C: RCPT TO:<Jones@foo.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: Blah blah blah...
C: ...etc. etc. etc.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel
```

Figura 17 - Diálogo de envio de e-mail com o protocolo SMTP.

Para testar se o corpo da mensagem é enviado de forma plana (não criptografada), foi analisado o pacote de envio do corpo do e-mail. Como já mostrado na Figura 17, esse pacote é enviado logo após o servidor responder com o 354 à solicitação de envio dos dados da mensagem pelo cliente. Como mostrado na Figura 18, o corpo da mensagem é legível para qualquer pessoa que intercepte a mensagem. Portanto, o protocolo SMTP não responde ao requisito de confidencialidade. Analisando o protocolo, concluí-se que um espião pode facilmente capturar e alterar o conteúdo de uma mensagem interceptada. Logo, os requisitos de integridade e autenticidade também não são atendidos.

Como citado na própria RFC 2821 [KLENSIN01] o protocolo SMTP é inerentemente inseguro e não deve ser utilizado em ambientes que requeiram segurança. A RFC também cita que e-mails com o corpo seguro são obtidos somente com o uso de aplicações extras, como o PGP (*Pretty Good Privacy*), ou com o protocolo S/MIME.

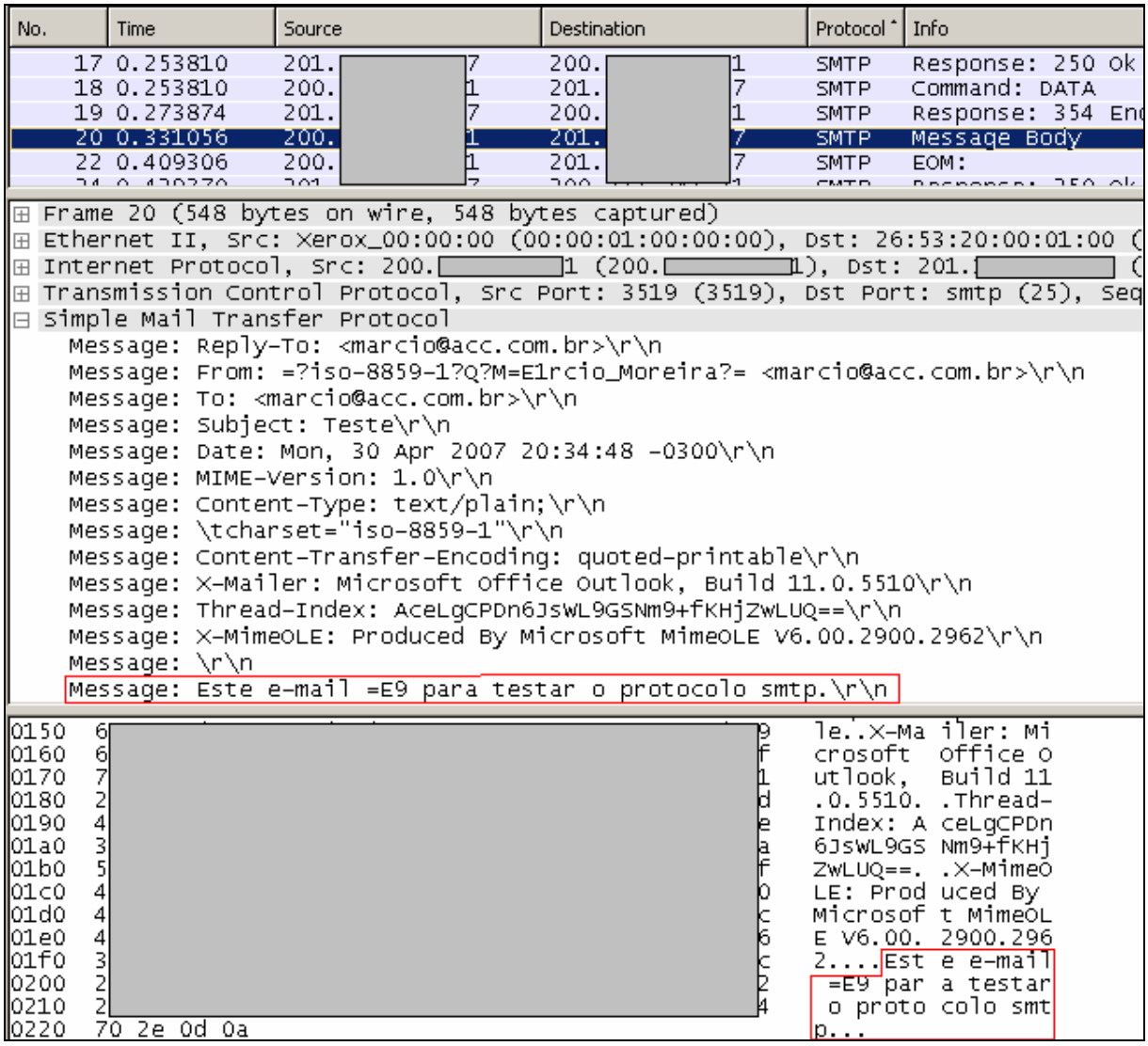

Figura 18 - Envio de corpo de e-mail com o protocolo SMTP.

3.2. POP3 (Post Office Protocol version 3)

O protocolo POP3 é também um padrão de fato nas recepções de e-mail na Internet. Ele foi definido na RFC 1225 (http://tools.ietf.org/html/rfc1225), substituída depois pela RFC 1460 (http://tools.ietf.org/html/rfc1460), que também foi substituída pela RFC 1725 (http://tools.ietf.org/html/rfc1725), que por sua vez também foi substituída pela RFC 1939 [M&ROSE96], que é utilizada como base nesse trabalho. A RFC 1939 foi atualizada pelas RFC 1957 (http://tools.ietf.org/html/rfc1957) e 2449 (http://tools.ietf.org/html/rfc2449).

Esse protocolo é utilizado para receber mensagens do MAA, do servidor onde o receptor tem conta de e-mail, para seu MUA. Uma vez recebida a mensagem, ela é apagada no servidor onde está o MAA. O padrão de autenticação do protocolo POP3 é inseguro, pois a

credencial passa em texto plano. Algumas implementações permitem o comando APOP, que fornece autenticação segura. Entretanto, mesmo que exista segurança durante a autenticação, durante a recepção das mensagens o protocolo POP3 não prevê nenhuma segurança.

Para testar as afirmações, foi enviada uma mensagem e, durante a recepção utilizando o protocolo POP3, verificada a autenticação e o corpo da mensagem. Como esperado, a autenticação foi feita em texto plano, sendo muito fácil obter a credencial (usuário e senha). O corpo da mensagem também foi transmitido em texto plano como mostra a Figura 19. Logo, analogamente ao protocolo SMTP, o protocolo POP3 não atende aos requisitos de confidencialidade, integridade e autenticidade.

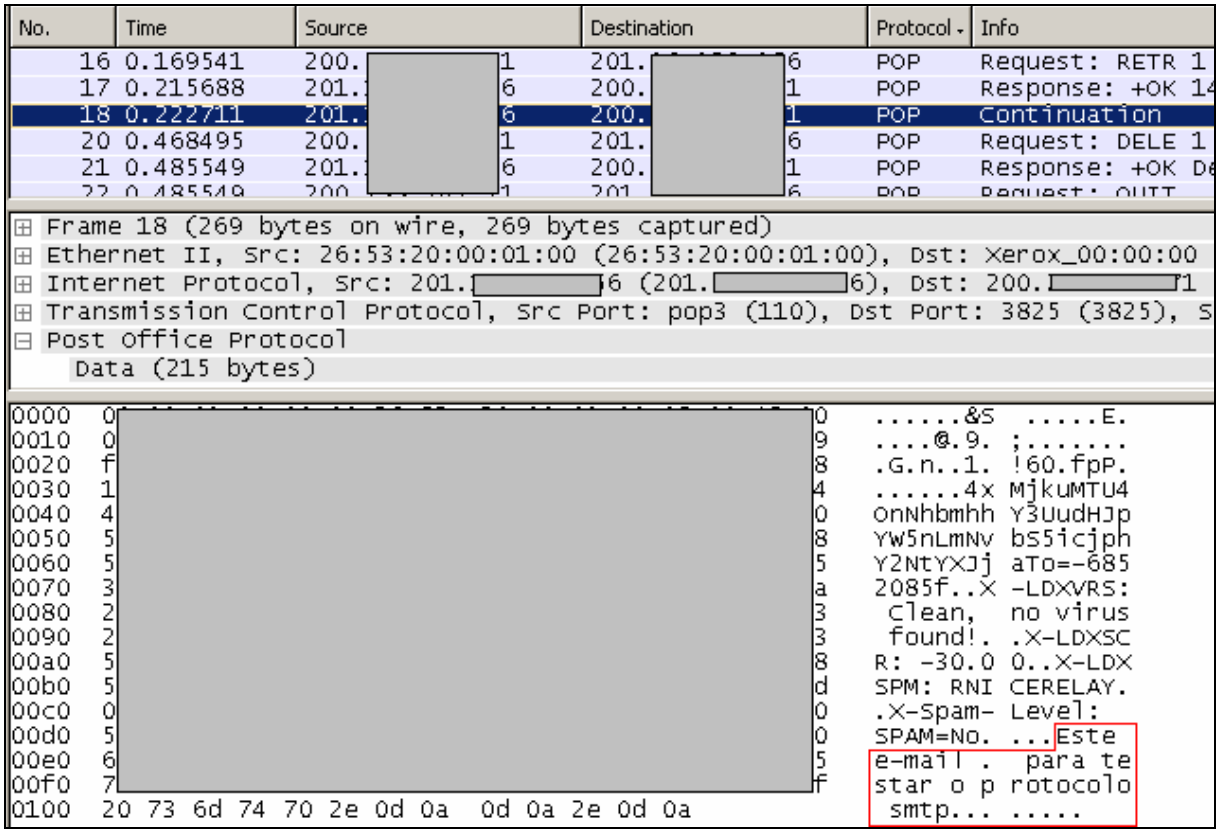

Figura 19 - Recepção de corpo de e-mail com o protocolo POP3.

3.3. IMAP (Internet Message Access Protocol)

A versão 4 do protocolo IMAP foi definida na RFC 1730 (http://tools.ietf.org/html/rfc1730), substituída depois pelas RFC 2060 (http://tools.ietf.org/html/rfc2060) e complementada pela RFC 2061 (http://tools.ietf.org/html/rfc2061). A RFC 2060 por sua vez foi substituída pela RFC 3501 (http://tools.ietf.org/html/rfc3501) [M&ROSE96], que é utilizada como base nesse

trabalho. A RFC 3501 foi atualizada pelas RFC 4466 (http://tools.ietf.org/html/rfc4466), RFC 4469 (http://tools.ietf.org/html/rfc4469) e RFC 4551 (http://tools.ietf.org/html/rfc4551).

O protocolo IMAP é utilizado para receber mensagens de um MAA para o MUA. A vantagem do IMAP sobre o POP3 é que ele permite baixar somente o cabeçalho da mensagem. O corpo da mensagem só é baixado se o usuário solicitar. Quanto uma mensagem grande (não desejada num determinando momento) antecede várias mensagens pequenas (necessárias naquele momento), o protocolo IMAP é bem mais interessante que o POP3 para gerenciar esta situação. Outra característica padrão do IMAP é que a mensagem seja baixada para a máquina local do usuário, sem excluir a mensagem no servidor. O POP3 também oferece esse recurso, porém esta não é a configuração padrão do protocolo. Se o usuário desejar este recurso, ele precisa marcar o parâmetro “deixar cópia das mensagens no servidor”. Assim o usuário pode ter acesso às mensagens de sua conta de e-mail de vários locais, até mesmo com ferramentas Webmail, que permitem visualizar as mensagens utilizando navegadores como o Internet Explorer, Mozilla, Firefox, etc. O IMAP também permite o compartilhamento de caixas postais por membros de um mesmo grupo de trabalho.

Como descrito na RFC 3501 [M&ROSE96], o protocolo IMAP permite a autenticação segura. Foram testados dois provedores que oferecem esse protocolo e foi visto que ambos não oferecem a facilidade da autenticação segura. Assim, por padrão, se não for negociado nenhuma forma de proteção, tanto a autenticação quanto os dados da mensagem são enviados como texto plano. O foco de segurança oferecido pelo protocolo IMAP é somente na autenticação. Para o corpo da mensagem o protocolo não especifica nada. Alguns provedores permitem que a conexão IMAP seja encapsulada pelo SSL (*Secure Sockets Layer*). Porém, esse recurso não é tão comum. Nesse caso, mesmo garantindo a confidencialidade por um recurso externo, o protocolo em si não garante nenhum dos aspectos de segurança.

Para testar o protocolo IMAP, foi enviada uma mensagem e verificada a autenticação e o corpo da mensagem durante a recepção utilizando o protocolo IMAP. Como esperado, a autenticação foi feita em texto plano, sendo muito fácil obter a credencial (usuário e senha). O corpo da mensagem também foi transmitido em texto plano como mostra a Figura 20. Logo, analogamente ao protocolo POP3, o protocolo IMAP não atende aos requisitos de confidencialidade, integridade e autenticidade.

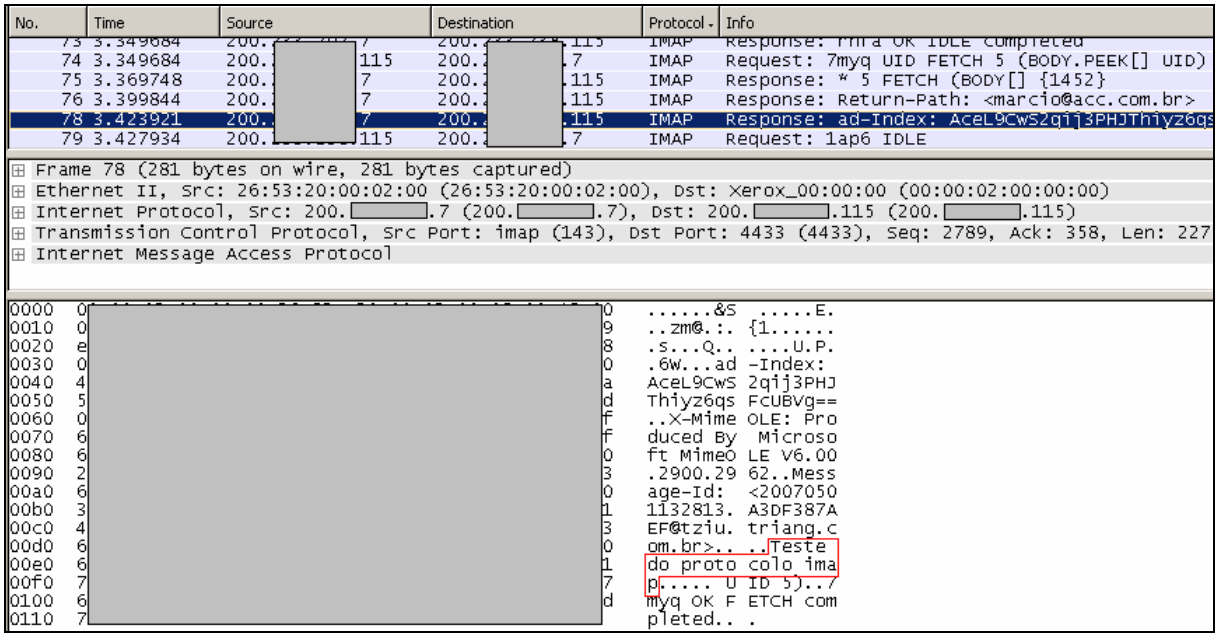

Figura 20 - Envio de corpo de e-mail com o protocolo IMAP.

3.4. S/MIME (Secure / Multipurpose Internet Mail Extensions)

A versão mais recente do S/MIME é a versão 3. Ela foi definida em cinco RFC. A RFC 2631 (www.ietf.org/rfc/rfc2631.txt) que trata do algoritmo de troca de chaves. A RFC 3370 (www.ietf.org/rfc/rfc3370.txt) que trata dos algoritmos de criptografia utilizados nas mensagens. A RFC 3850 (www.ietf.org/rfc/rfc3850.txt) que trata do manuseio dos certificados digitais. A RFC 3851 (www.ietf.org/rfc/rfc3851.txt) [RAMSDELL04] que trata da especificação das mensagens que utilizam esse protocolo, sendo essa RFC utilizada como base nesse trabalho. Finalmente a RFC 3852 (www.ietf.org/rfc/rfc3852.txt) que trata da parte sintática da criptografia das mensagens.

O protocolo S/MIME foi desenvolvido pela empresa RSA Data Security Inc. Segundo os proponentes, ele foi feito para enviar e receber dados seguros no formato MIME. Esse protocolo é baseado no formato de mensagens PKCS #7 (*Public-Key Cryptography Standards*, padrões de criptografia de chave-pública) e no formato de certificados X.509v3. Desta forma, o protocolo permite cifrar e assinar mensagens a serem enviadas, assim como decifrar e verificar assinaturas de mensagens recebidas. Conseqüentemente têm-se os seguintes recursos de segurança com esse protocolo: autenticidade, integridade, não repúdio de origem (para mensagens assinadas) e confidencialidade (para as mensagens cifradas) [RAMSDELL04]. Diante disto, se estas informações forem verdadeiras, esse protocolo atende aos requisitos de segurança desejados.

Uma abordagem importante que foi utilizada na construção desse protocolo é que ele foi construído para ser utilizado “fim a fim” (*end-to-end*). Em outras palavras, a assinatura e a cifragem são aplicadas no MUA do emissor, a decifragem e a verificação da assinatura são feitas no MUA do receptor. Os MTAs, MDA e MAA envolvidos, não precisam se preocupar nem tratar nenhum aspecto do protocolo S/MIME, pois para eles é uma mensagem comum que está sendo enviada. Assim, somente o receptor pode ler a mensagem e verificar a assinatura do emissor na mesma. Tudo o que era necessário para fazer isto já era conhecido há muito tempo. Mas a RFC para aplicação desses recursos de forma eficiente aos e-mails foi publicada somente em 2004.

Os requisitos de segurança propostos são atendidos por dois métodos: S/MIME e PGP (nas suas duas implementações o PGP/MIME e o novo OpenPGP) [CHAU05], [R&KORVER03] e [NGSS06]. Os protocolos propostos anteriormente PEM (*Privacy Enhanced Mail*) e MOSS (*MIME Object Security Services*) não ganharam adesões significativas no mercado [HOFFMAN04]. Por outro lado, o S/MIME ganhou implementações importantes da Microsot, Netscape e outros. O PGP está crescendo no mundo livre. Entretanto, os dois métodos utilizam o MIME como base para cifragem, agregação de assinatura e autenticação, as variações ficam por conta dos formatos e algoritmos.

A Figura 21 reproduz uma comparação dos métodos S/MIME e do OpenPGP feita no artigo “*S/MIME and OpenPGP*” de Paul Hoffman de 2004 [HOFFMAN04]. Outra comparação pode ser vista no artigo “*Electronics mail security (PGP & S/MIME)*” [PATELCJ01]. Os dois métodos são relativamente equivalentes. Entretanto, o PGP utiliza formatos proprietários enquanto o S/MIME padrões reconhecidos pelo mercado. Diante do exposto, será testado apenas o protocolo S/MIME.

Recursos	**S/MIME v3**	**OpenPGP**
Formato da mensagem	Binário, baseado no CMS	Binário, baseado no PGP
Formato do certificado	Binário, baseado no X.509v3	Binário, baseado no PGP
Algoritmo de cifragem	TripleDES (DES EDE3 CBC)	TripleDES (DES EDE3 CFB)
Algoritmo de assinatura	Diffie-Helmman (X9.42) com DSS ou RSA	ElGamal com DSS
Algoritmo *hash*	SHA-1	SHA-1
Encapsulamento MIME de dados assinados	Multipartes assinadas ou Formato CMS	Multipartes assinadas com ASCII armor
Encapsulamento MIME de dados cifrados	Aplicação do PKCS7-MIME	Multipartes cifradas

Figura 21 - Comparação S/MIME v3 e OpenPGP.

Para testar o protocolo S/MIME foi enviada uma mensagem assinada e criptografada digitalmente. Foi monitorado o envio e a recepção da mesma. A autenticação nesse protocolo é segura por definição. A Figura 22 mostra, na interceptação do envio, o começo do corpo da mensagem identificando o remetente, o destinatário e o assunto. Também foi destacado o formato da mensagem e a base de codificação. Finalmente, foi destacado o corpo da mensagem em si, note que esse é ilegível a um espião.

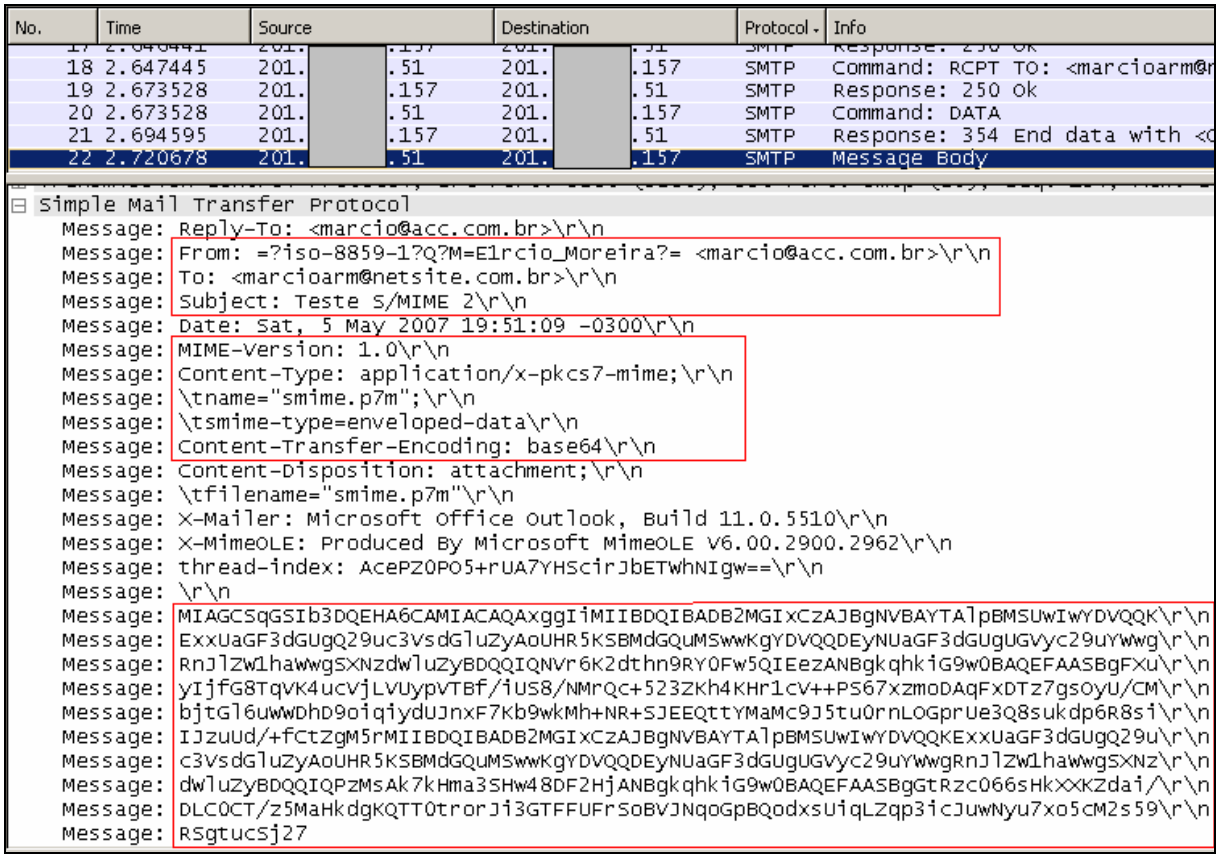

Figura 22 - Envio de corpo de e-mail com o protocolo S/MIME.

A Figura 23 mostra o aviso do Outlook Express ao receber a mensagem assinada e criptografada digitalmente com o S/MIME.

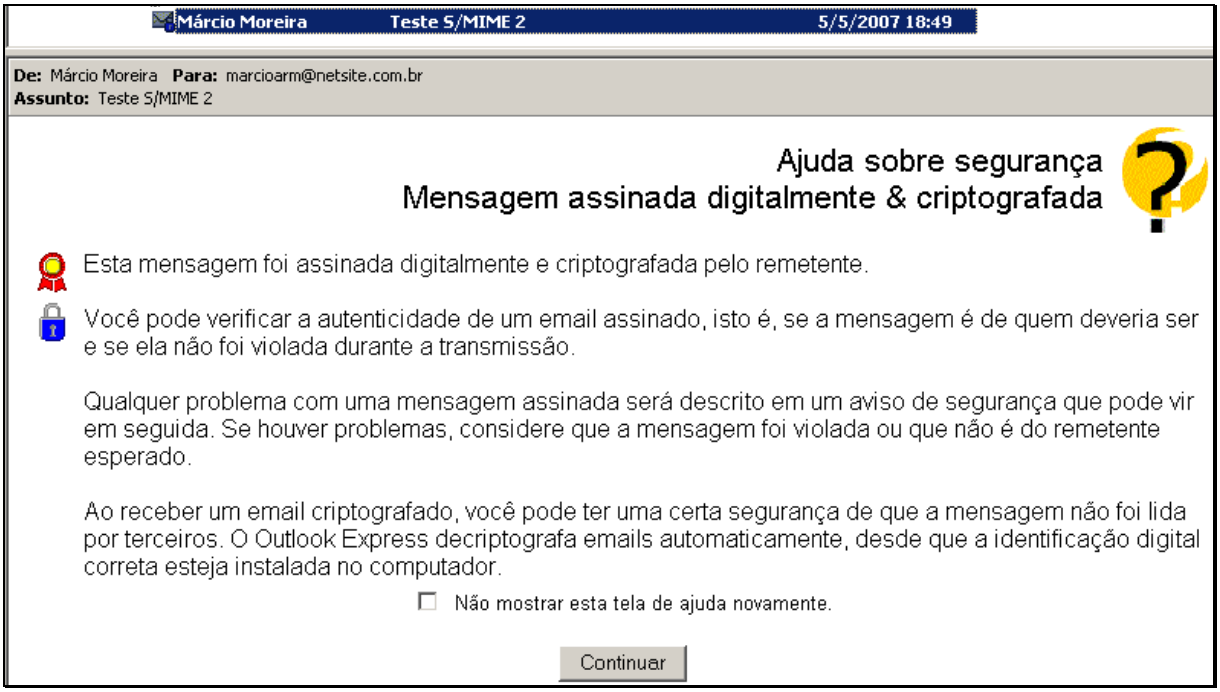

Figura 23 - Alerta de mensagem assinada e criptografada no Outlook Express.

Para ver a mensagem propriamente dita, clica-se no botão “Continuar” do aviso do Outlook Express e então é mostrada a mensagem como apresentado na Figura 24.

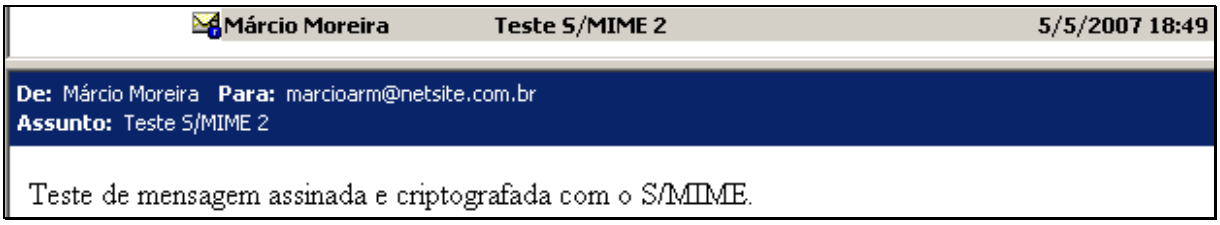

Figura 24 - Mensagem decifrada e com assinatura verificada no Outlook Express.

Como o S/MIME é um protocolo ponto a ponto, sua adoção deve passar por alguns estágios. Os usuários podem incluir filtros em seus MUA para eliminar ou mover as mensagens não assinadas para pastas especiais. Os provedores de serviços de e-mail também passarão a adotar políticas que minimizem a geração de *spams* em seus domínios, pois poderão ser responsabilizados por isto. Da mesma forma os provedores de serviço dos receptores de *spams* também poderão adotar políticas que reduzirão estas mensagens, por exemplo, disponibilizando regras de eliminação de mensagens cuja origem não possa ser comprovada. No âmbito corporativo, os administradores de sistemas poderão criar regras semelhantes às citadas anteriormente para todos os usuários sob sua responsabilidade. Estas regras podem inclusive fazer parte da política de segurança da corporação.

3.5. SPF (Sender Policy Framework)

O SPF foi definido na RFC 4408 (www.ietf.org/rfc/rfc4408.txt) [WONG&S06]. Esta RFC foi publicada em Abril de 2006 junto com as RFC 4405 (www.ietf.org/rfc/rfc4405.txt), 4406 (www.ietf.org/rfc/rfc4406.txt) e 4407 (www.ietf.org/rfc/rfc4407.txt). Como está dito nas próprias RFC, elas são um conjunto de documentos publicados simultaneamente como RFC experimentais, ainda não existe consenso nem esforços de alinhamento das abordagens propostas.

O SPF é uma extensão do SMTP, que permite ao MTA identificar e rejeitar mensagens cujo Endereço de Retorno (Return-Path) seja forjado. Naturalmente, os *spammers* forjam ou não preenchem o endereço de retorno. Para que o SPF gere os efeitos desejados são necessárias duas ações:

1) No domínio emissor, definir e publicar a política de envio de mensagens:

   O administrador do domínio emissor do e-mail deve designar quais máquinas estão autorizadas a enviar mensagens em nome do domínio sob sua responsabilidade.

2) No domínio receptor, estabelecer critérios de aceitação das mensagens:

   O administrador do domínio receptor do e-mail deve habilitar a checagem do SPF no MTA e definir o que será feito com as mensagens não aprovadas.

A publicação da política é independente da verificação da mensagem. Quando uma mensagem estiver sendo verificada pelo MTA, o SPF poderá retornar os caracteres:

- "+" - *Pass*: O IP de retorno está autorizado a enviar mensagens em nome do domínio emissor. O domínio receptor pode aceitar a mensagem.
- "-" - *Fail*: O IP de retorno não está explicitamente autorizado a enviar mensagens em nome do domínio. O domínio receptor pode rejeitar a mensagem ou marcá-la para uma revisão rigorosa.
- "?" - *Neutral*: O domínio emissor não está com o SPF habilitado ou não tem como definir se o IP de retorno está autorizado ou não a enviar mensagens em seu nome. O domínio receptor não pode rejeitar a mensagem baseado no SPF, pois esse não conseguiu confirmar ou rejeitar o IP de retorno.

- "~" - *Softfail*: O domínio emissor acha que o IP de retorno não está autorizado, mas não pode afirmar com segurança. Esta resposta é utilizada quando o SPF está em fase de implantação. Esta resposta deve ser tratada pelo domínio receptor da mesma forma que o *neutral*.

O SPF acrescenta ao SMTP a possibilidade de confirmação de que o endereço de retorno pertence ao domínio emissor. Logo, ele é uma forma de lista branca (*white list*). Sem dúvida o SPF representa um esforço em direção à redução do volume de *spams*. Mas, ele depende de implementações adicionais (tanto no domínio emissor quanto no domínio receptor) e assim como o SMTP, ele não garante confidencialidade (não cifra a mensagem), integridade (a mensagem pode ser alterada) e nem autenticidade, pois a mensagem não estará assinada digitalmente. Mesmo que o endereço de retorno pertença ao domínio emissor, tanto o IP quanto o endereço de e-mail do emissor podem ter sido "plantados" na mensagem. Portanto, o SPF também não atende aos requisitos de segurança propostos.

3.6. DKIM (DomainKeys Identified Mail)

O DKIM foi definido na RFC 4870 (www.ietf.org/rfc/rfc4870.txt) por M. Delany, foi aprovado como uma proposta padrão pelo IETF em Fevereiro de 2007 e publicado em Maio de 2007. Esta RFC foi redefinida pela RFC 4871 (www.ietf.org/rfc/rfc4871.txt) [DELANY07], também publicada em Maio de 2007, num esforço conjunto de pessoas da Sendmail Inc., PGP Corporation, Yahoo! Inc. e Cisco Systems, Inc. O projeto do DKIM está descrito na página: www.dkim.org.

No DKIM, o domínio emissor adiciona o nome do domínio e a assina digitalmente a mensagem. A mensagem é assinada por um *Administrative Management Domain* (ADMD), no domínio do emissor, e pode ser feita pelo MUA, MTA ou *Mail Submission Agent* (MSA). O DKIM também permite que a assinatura seja feita por um procurador autorizado. A validação da assinatura pode ser feita por qualquer agente de e-mail entre o MTA do emissor e o MAA do receptor. A RFC prevê que esta validação seja feita pelo ADMD do servidor do receptor da mensagem, para que o MUA do receptor não precise realizar esse trabalho.

No DKIM, quando o administrador do domínio do emissor adiciona seu nome de domínio à mensagem e a assina, ele se torna responsável pela conta de e-mail do emissor. Ele também se torna co-responsável pela origem da mensagem, não podendo negar sua

origem. A assinatura da mensagem garante a integridade da mensagem (do MTA do emissor até o MAA do receptor) e autenticidade de domínio emissor.

O DKIM é uma boa implementação de listas brancas (*white list*). Ele dá aos administradores de domínio a chance de isolar domínios geradores de *spam*. Como ele foi feito por um consórcio de empresas (Sendmail, PGP, Yahoo e Cisco) fortes e influentes na questão de e-mails sua adoção deve ser grande e rápida. O mais importante é o movimento claro da comunidade da Internet no sentido de reduzir os *spams*. A indignação com os *spams* já está declarada por toda a comunidade.

Como mostra a Figura 25 existem dois pontos vulneráveis no protocolo DKIM. O tráfego da mensagem do MUA do emissor até o MTA de seu servidor de domínio e o tráfego entre o MAA e o MUA do receptor. No primeiro, a mensagem ainda não foi assinada digitalmente e no segundo a mensagem já foi verificada e a assinatura digital removida. Em ambos os pontos a mensagem pode ser interceptada e alterada, isto fragiliza o sistema. O DKIM não garante confidencialidade. A autenticidade está limitada ao domínio do emissor e assim como a integridade, ambas são garantidas somente do MTA do emissor até o MAA do receptor. Mas, não estão garantidas no MUA do emissor e nem do receptor. Portanto, o protocolo DKIM também não atende aos requisitos de segurança propostos.

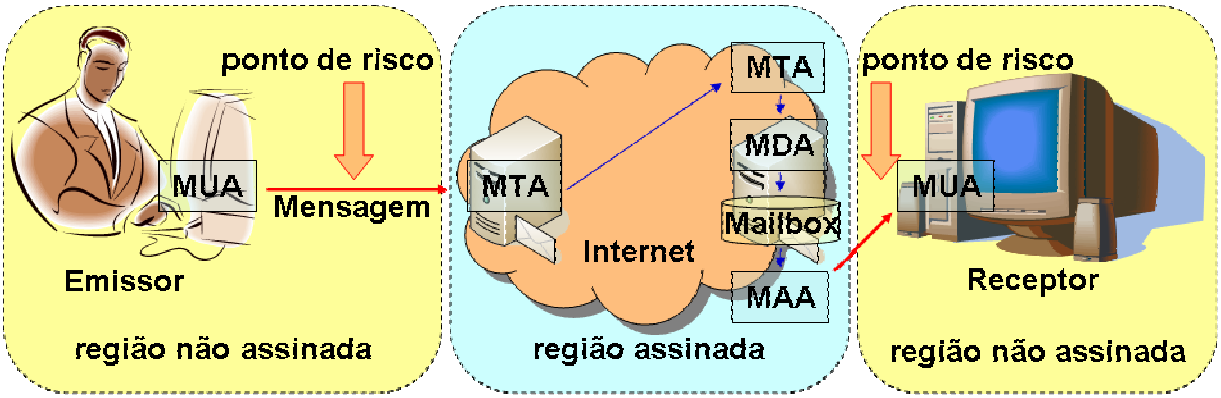

Figura 25 - Pontos de risco do protocolo DKIM.

4. Como utilizar o protocolo S/MIME

O propósito do capítulo anterior era confirmar ou refutar a hipótese de que “deve existir um protocolo que permita o uso de e-mails seguros”. Com as análises realizadas, concluiu-se que o protocolo S/MIME confirmou esta hipótese de pesquisa. Diante disto, este capítulo é dedicado à descrição de como utilizar este protocolo para o envio e recepção de mensagens seguras.

4.1. Necessidades dos provedores de serviço de e-mail

Como o protocolo S/MIME foi construído para ser utilizado “fim a fim”, somente os MUA do emissor e do receptor precisam tratar a assinatura digital e a cifragem. Consequentemente os provedores de serviços de e-mail não precisam dedicar nenhum tratamento especial ao protocolo. Eles apenas precisam suportar o protocolo MIME que é utilizado pelo S/MIME.

Entretanto, para os provedores ou administradores de serviço de e-mail é primordial a configuração de ambientes seguros, conforme recomendações de melhores práticas de mercado. Nesse sentido, o conhecimento dos textos a seguir é fundamental para estes provedores e administradores:

- Para os usuários de softwares livres do mundo Linux e Unix:
  - “*Utilizing Open-Source Software to Build a (Relatively) Secure, Spam- and Virus-Free Mail Service*”, escrito em 2004 por David Bailey [BAILEY04].
  - “*Segurança em Servidores de Correio Eletrônico*“, escrito por Marcel Souza em 2006 [SOUZA06].
- Para os usuários do Microsoft Exchange, recomenda-se ler os artigos na página do Technet da Microsoft: http://technet.microsoft.com/pt-br/library/aa996058.aspx, mais especificamente o artigo “*The Changing Landscape of E-mail Security*“, disponível em: http://technet.microsoft.com/pt-br/library/aa995984.aspx.
- Para os usuários do IBM Lotus Notes, recomenda-se o RedBook sg247017, conforme recomendação da IBM em “*Lotus Security Handbook*”, disponível em: www.redbooks.ibm.com/abstracts/SG247017.html.

Naturalmente, esses não são os únicos textos a respeito do assunto. O objetivo de citá-los é apenas chamar a atenção dos administradores para as necessidades de segurança.

4.2. Necessidades dos usuários de serviço de e-mail

Um usuário de e-mail para enviar mensagens assinadas e/ou cifradas precisa:

1) Obter um certificado digital.
2) Instalar seu certificado digital.
3) Publicar seu certificado digital.

4.2.1. Obtendo um certificado digital

Como mencionado na seção 2.1.4. Certificação Digital, a obtenção de um certificado digital, tanto para pessoa física quanto jurídica, deve ser feita em uma Autoridade Certificadora (CA) Credenciada pela ICP-Brasil. Seguem algumas CA autorizadas pelo ICP-Brasil e SRF:

- Credenciadas pelo próprio ICP-Brasil:
  - CertiSign: www.certisign.com.br.
  - Serasa: www.serasa.com.br.
  - Imesp: www.imesp.com.br (parcerias: SRF, CertiSign e VeriSign).
  - Prodemge: www.prodemge.gov.br (parceria com a SRF).
  - CEF: https://icp.caixa.gov.br.
- Credenciadas pelo e-CAC da SRF (www.receita.fazenda.gov.br):
  - ACSerpro-SRF: https://ccd.serpro.gov.br/certificados/.
  - ACCertSign-SRF: www.certisign.com.br/receita/.
  - ACSerasa-SRF: www.serasa.com.br/certificados/receitafederal.htm.

Existem dois tipos de certificados o A1 e o A3. No certificado do tipo A1, as chaves (pública e privada) são geradas no computador do solicitante. No certificado do tipo A3, as chaves são geradas em um hardware específico (*token*, *smart card*, etc.) que não permite a exportação, reprodução ou cópia da chave privada. Em ambos os casos a chave pública é enviada à CA enquanto a chave privada permanece em poder do solicitante protegida por senha no tipo A1 ou pelo hardware no tipo A3. O certificado obtido da CA do tipo A1 tem validade de um ano e é instalado no mesmo computador onde a solicitação foi feita. O certificado do tipo A3 tem validade de 3 anos e pode ser instalado no hardware onde está a chave privada ou em outro equipamento. O certificado do tipo A3 é mais seguro que o A1.

As Autoridades Certificadoras credenciadas pela SRF emitem o e-CPF e o e-CNPJ, que são respectivamente o certificado digital para pessoas físicas (Cadastro de Pessoas Físicas) e jurídicas (Cadastro Nacional de Pessoas Jurídicas). Em julho de 2007, o e-CPF custava de R$90,00 a R$475,00 dependendo do tipo de certificado (A1 ou A3) e acessórios (cartão com chip, token ou cartão para notebook). O e-CNPJ custava de R$130,00 a R$550,00 dependendo do tipo (A1 ou A3) e acessórios.

Além do e-CPF e e-CNPJ existem também outros certificados:

- Para empresas:
    - Assinatura de documentos.
    - Assinatura de notícias.
    - Certificados para servidores.
    - E-Mail seguro corporativo (o custo depende da quantidade de usuários).
    - IMS (*Identity Management System* ou Sistema de Gerenciamento de Identidades Digitais).
    - PKI (*Public Key Infrastructure* ou Infra-estrutura de Chave Pública).
    - Notebook corporativo seguro.
    - SDK (*Software Development Kit* ou Kit para Desenvolvimento de Software).
    - SPB (Sistema de Pagamentos Brasileiro).
    - Workflow (fluxos de trabalho).
    - CertJUS (certificados para o sistema jurídico brasileiro).
    - WinLogon (autenticação no Windows).
- Para pessoas físicas:
    - Assinatura de documentos.
    - Notebook pessoal seguro.
    - E-Mail pessoal seguro (custa em torno de R$50,00 para um ano).

Para ambientes de e-mail corporativo, uma opção é o Certificado Digital para e-mail seguro corporativo. Nesta modalidade a corporação pode emitir certificados para seus usuários. Pela aquisição de uma licença para emissão de vários certificados de uma vez, o custo por certificado deveria ser menor. Mas, nas entidades credenciadas pesquisadas isto não ocorre. Por exemplo, na CertiSign o certificado de e-mail corporativo para 100 usuários sai por R$123,33 por certificado, enquanto o certificado para e-mail pessoal seguro sai por R$46,00. Logo, a melhor relação custo-benefício é obtida com a aquisição um certificado de e-mail pessoal seguro para cada usuário.

Alternativamente às Autoridades Certificadoras Credenciadas, as empresas de menor porte podem optar por soluções não credenciadas, tais como: CeSigner (www.qualisoft.com.br) e SafeWeb (www.safeweb.com.br). Outra opção é a instalação de uma autoridade certificadora na própria empresa. Nesse caso a empresa cria, distribui e administra certificados. Existem várias soluções livres, inclusive no próprio Windows, para esta finalidade. O lado negativo das opções livres e autoridades não credenciadas é a falta de compatibilidade com outras corporações.

Para o usuário que não quer ou não pode pagar por um certificado, a opção mais utilizada em todo o mundo é a Thawte (www.thawte.com), que permite a geração de certificados sem custos que são compatíveis com a maioria dos MUA existentes atualmente (Outlook, Outlook Express, Lotus Notes, etc.). Os certificados utilizados nesse trabalho foram gerados pela Thawte.

4.2.2. Instalando um certificado digital

Ao receber um certificado digital, o emissor envia, além do certificado digital solicitado, um conjunto de certificados digitais dele e das demais Autoridades Certificadoras até chegar ao certificado digital da Autoridade Certificadora Raiz. A Figura 26 mostra uma árvore com três níveis de certificados, desde o certificado raiz, passando pelo da Autoridade Certificadora e terminando com o do usuário. A instalação dos certificados deve ser feita nesta ordem, da raiz para o usuário.

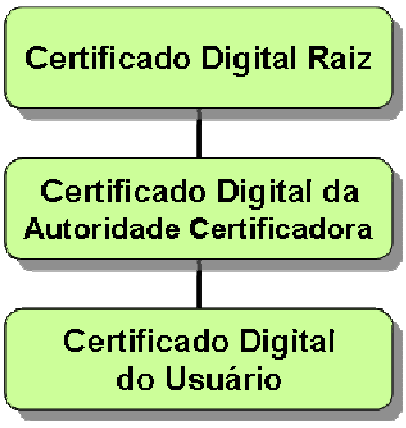

Figura 26 - Árvores de certificados digitais.

Nesse trabalho é descrito como instalar certificados no ambiente Windows XP e no MUA Outlook. Para outros ambientes ou MUA, o interessado poderá adequar as instruções aqui

mencionadas, procurar materiais específicos ou recorrer à documentação do Sistema Operacional ou MUA utilizados.

a) Instalando o certificado raiz e da autoridade certificadora

A autoridade certificadora envia o certificado raiz e o certificado dela. Esses arquivos precisam ser instalados no centro de armazenamento de certificados do Windows. Salve os arquivos recebidos em uma pasta adequada e execute os procedimentos a seguir para o certificado raiz e depois para o certificado da autoridade certificadora.

1) No Internet Explorer selecione: **Ferramentas, Opções da Internet, Conteúdo, Certificados**. Como mostrado na Figura 27.

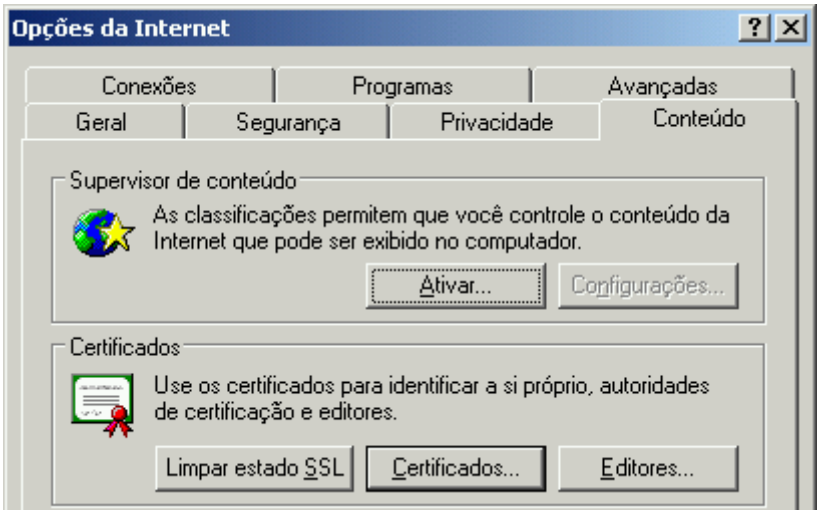

Figura 27 - Certificados no Internet Explorer.

2) Em Certificados selecione **Importar** e siga as instruções do assistente para importação de certificados. Como mostrado na Figura 28.

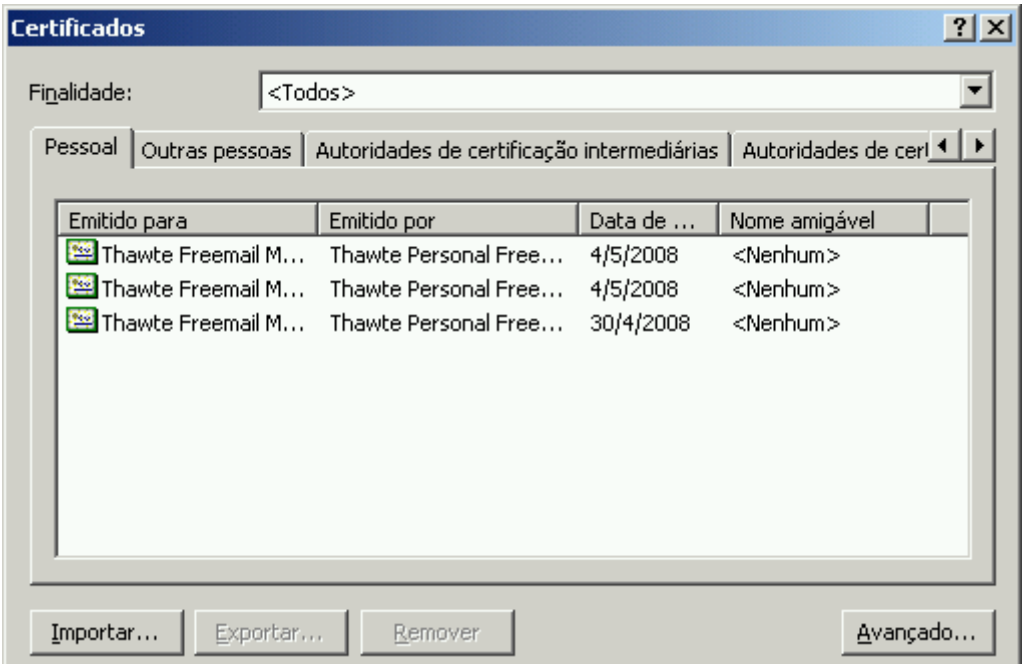

Figura 28 - Importação de certificados do Windows.

b) Instalando o certificado do usuário

A autoridade certificadora envia o certificado digital do usuário. É possível ter um certificado para assinar mensagens e outro para cifrar mensagens. Na prática, o mais comum é a utilização de um único certificado para as duas finalidades. Esses arquivos precisam ser instalados no MUA do usuário. Salve os arquivos recebidos em uma pasta adequada e execute os procedimentos a seguir:

1) No Outlook selecione: **Ferramentas, Opções, Segurança** e **Configurações**. Como mostrado na Figura 29.

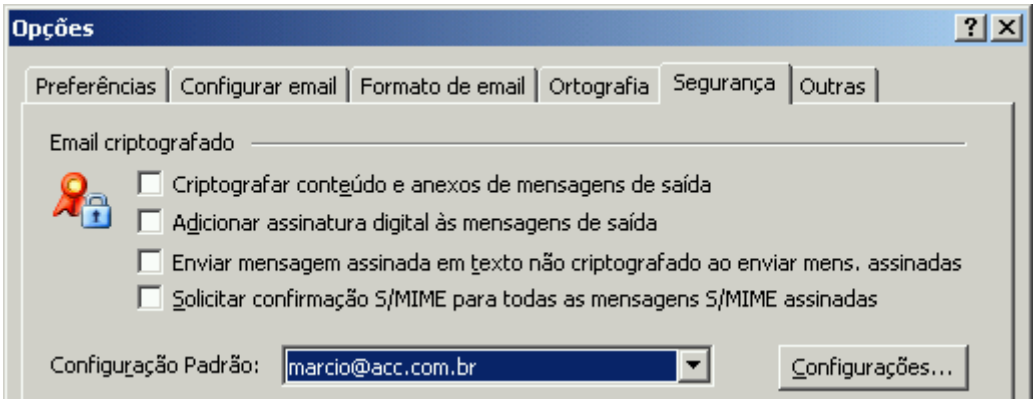

Figura 29 - Opções e configuração de segurança do Outlook.

2) Preencha as preferências de configurações como mostrado na Figura 30. No nome das configurações, use seu e-mail. Selecione o S/MIME e marque os dois checkbox.

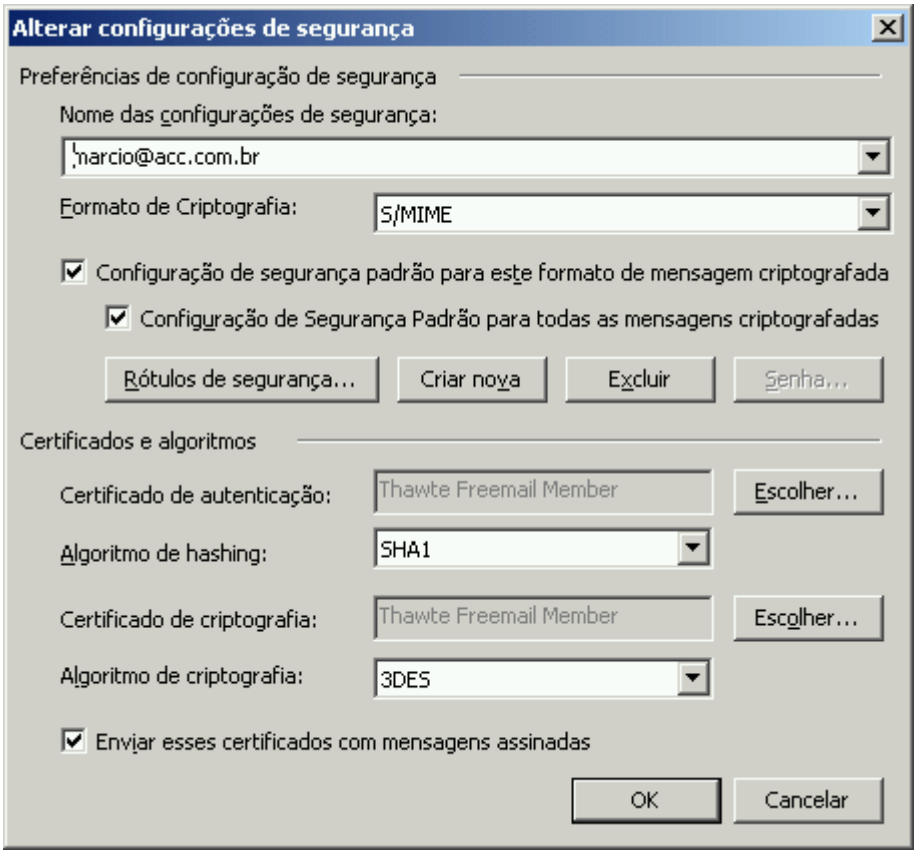

Figura 30 - Configurações de segurança do Outlook.

3) Na frente do certificado de autenticação clique no botão **Escolher**, escolha o certificado a ser utilizado para autenticação de mensagens e clique em **Ok**. Como mostrado na Figura 31.

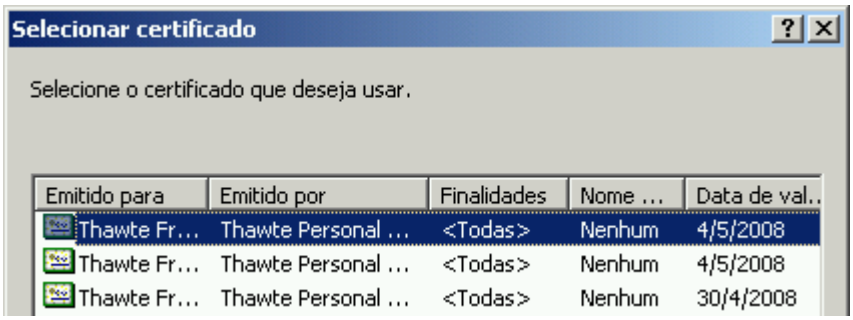

Figura 31 - Selecionando certificados no Outlook.

4) Da mesma forma, à frente do certificado de criptografia clique no botão **Escolher**, selecione o certificado a ser utilizado para cifrar mensagens e clique em **Ok**.

5) Certifique-se que o algoritmo de *hash* esteja definido como **SHA1**, o algoritmo de criptografia esteja definido como **3DES** e a opção “Enviar esses certificados com

mensagens assinadas" esteja marcada. Como já mostrado na Figura 30. Clique no botão **Ok**.

4.2.3. Publicando um certificado digital

Existem duas formas de publicar o certificado de um usuário. Enviando-o junto com mensagens assinadas ou enviando-o previamente para receber mensagens cifradas.

a) Enviando o certificado com mensagens assinadas

Como as mensagens são assinadas com a chave privada do usuário, o certificado contendo a chave pública pode ser enviado junto com a própria mensagem.

1) No Outlook selecione: **Ferramentas, Opções, Segurança** e **Configurações**. Como já mostrado na Figura 29.

2) Em Certificados e algoritmos, certifique-se que a opção "Enviar esses certificados com mensagens assinadas" esteja marcada. Como já mostrado na Figura 30. Clique no botão **Ok**.

b) Enviando o certificado previamente para receber mensagens cifradas

Como as mensagens são cifradas com a chave pública do destinatário, o certificado contendo esta chave precisa já estar disponível na MUA do emissor no momento de cifrar a mensagem. Logo, para enviar uma mensagem cifrada para um usuário chamado João, é necessário obter e instalar o certificado dele antes de enviar a mensagem. Peça que ele lhe envie o certificado dele, copie-o numa pasta temporária e execute os procedimentos:

1) No Outlook selecione **Contatos** e abra os dados do contato clicando duas vezes no nome dele. Como mostrado na Figura 32. Se o contato não existir, crie um.

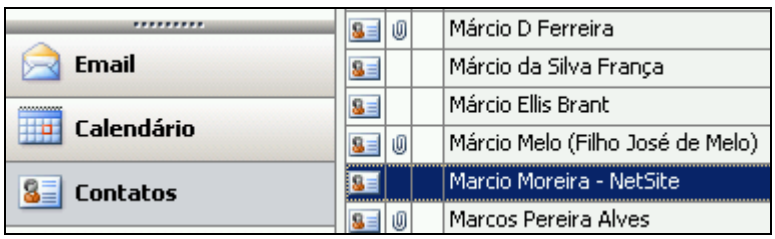

Figura 32 - Selecionando um contato no Outlook.

2) Nos detalhes do contato selecionado clique em **Certificado** e no botão **Importar**, como mostrado na Figura 33.

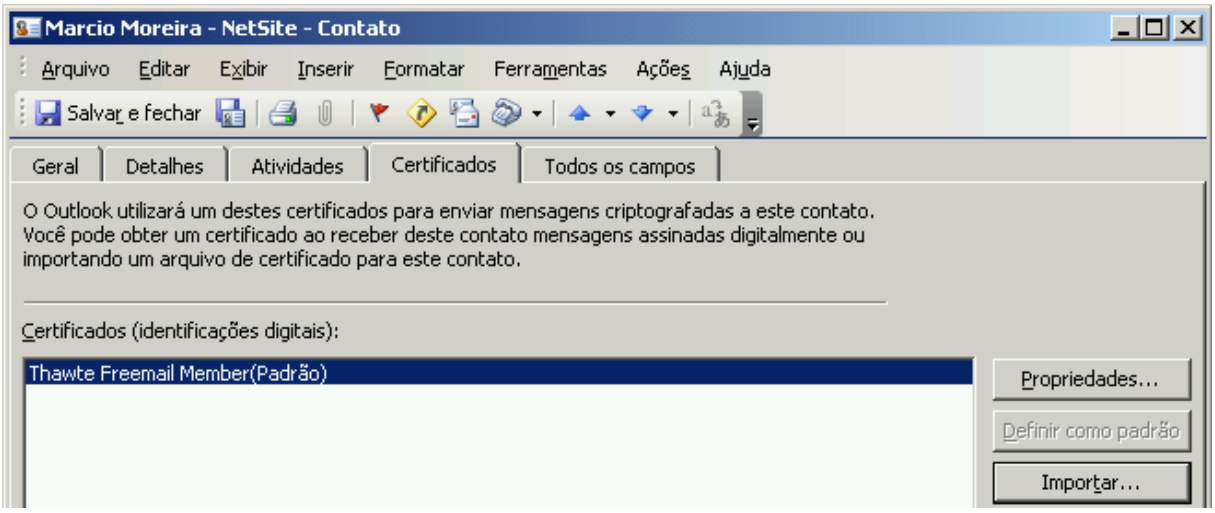

Figura 33 - Importando o certificado de um contato no Outlook.

3) Selecione e importe o certificado do usuário desejado.

Uma vez importado, o certificado pode ser apagado da pasta temporária. Nesse ponto, já é possível enviar uma mensagem cifrada para o usuário cujo certificado foi importado. Esse processo não precisa ser repetido enquanto não tiver nenhuma mudança no certificado do destinatário. A mensagem é cifrada com a chave pública dele e só poderá ser decifrada por ele, pois somente ele tem a chave privada. Se a mensagem for enviada a vários destinatários, todos eles devem ter seus certificados importados.

4.3. Enviando mensagens assinadas e cifradas

Para enviar mensagens assinadas e cifradas no Outlook, clique em nova mensagem normalmente, selecione os destinatários, digite o assunto e o corpo da mensagem.

1) Para assinar digitalmente a mensagem clique no botão de assinar (selo), como mostrado na Figura 34.

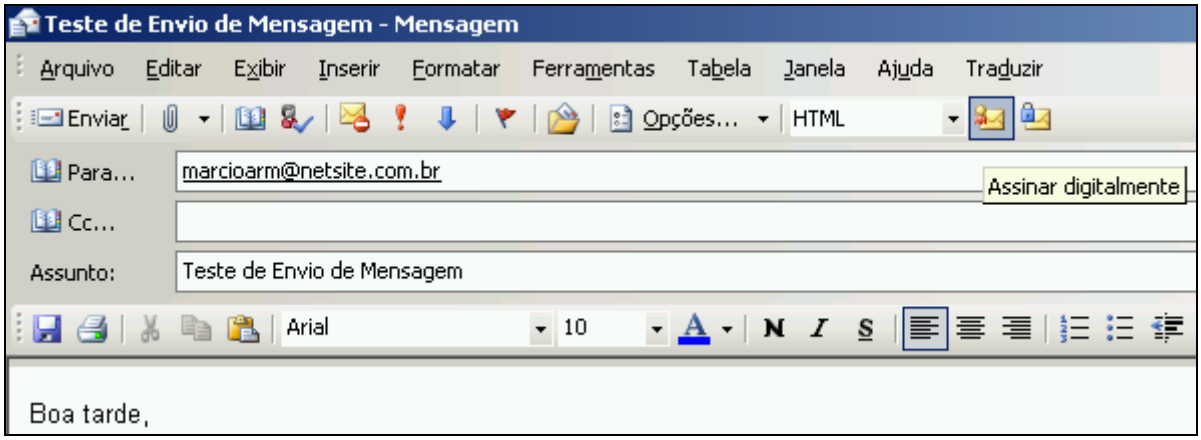

Figura 34 - Assinando mensagens no Outlook.

2) Para cifrar a mensagem clique no botão de cifrar (cadeado), como mostrado na Figura 35

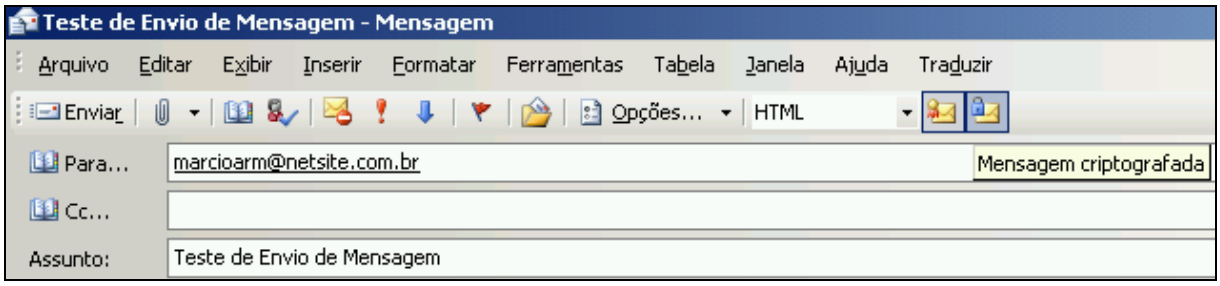

Figura 35 - Cifrando mensagens no Outlook.

3) Para acessar as opções completas de segurança da mensagem clique em **Opções** e **Configurações de segurança**, como mostrado na Figura 36.

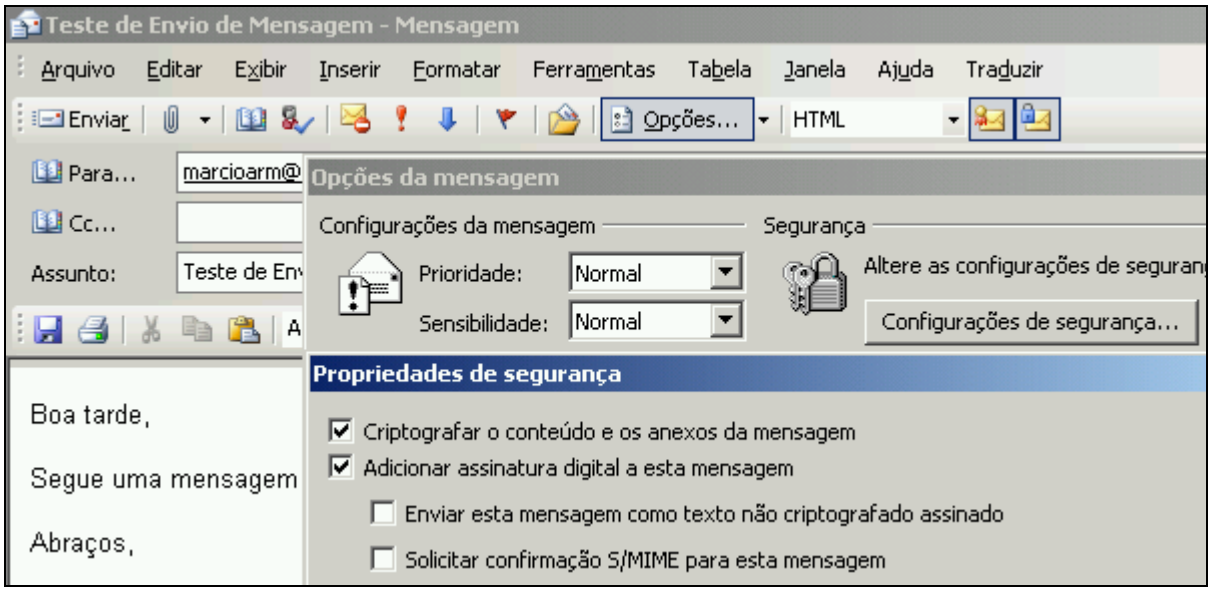

Figura 36 - Configurações de segurança de uma mensagem no Outlook.

4) Toda vez que uma mensagem cifrada for exibida, ela precisará ser decifrada. Para isto, o Outlook precisa acessar sua chave privada. Um alerta como o mostrado na Figura 37 é exibido. Para ver a mensagem, basta clicar no botão **Ok**.

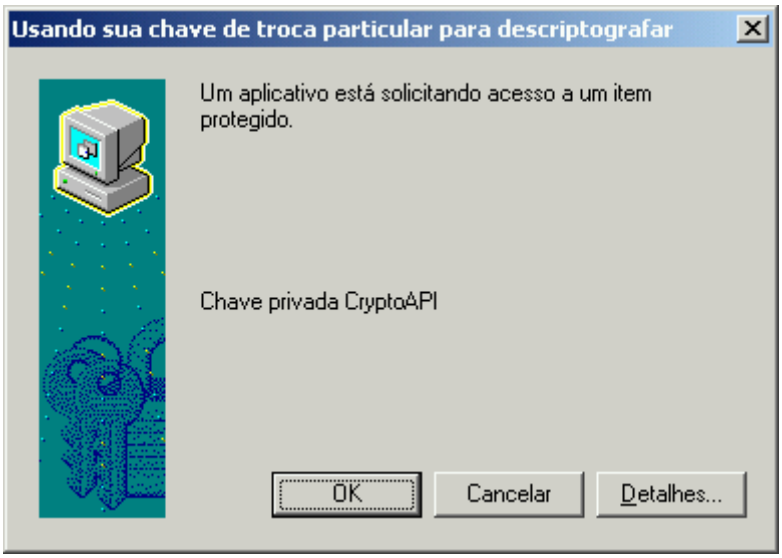

Figura 37 - Mensagem de alerta à chave privada do certificado no Outlook.

Essa mensagem ocorrerá toda vez que o Outlook precisar acessar a chave privada de um certificado para decifrar uma mensagem.

4.4. Recebendo mensagens assinadas e cifradas

As mensagens assinadas e cifradas serão recebidas normalmente pelo Outlook. Mas, não são exibidas no painel de visualização do Outlook.

1) Para abrir uma mensagem cifrada, dê um clique duplo na mensagem como mostrado na Figura 38.

Figura 38 - Recebendo mensagem cifrada no Outlook.

2) Ao abrir uma mensagem assinada, a assinatura é verificada. Se a mensagem for cifrada, ela é decifrada para ser exibida. O cadeado indica que a mensagem foi cifrada e o selo indica que ela foi assinada, como mostra a Figura 39.

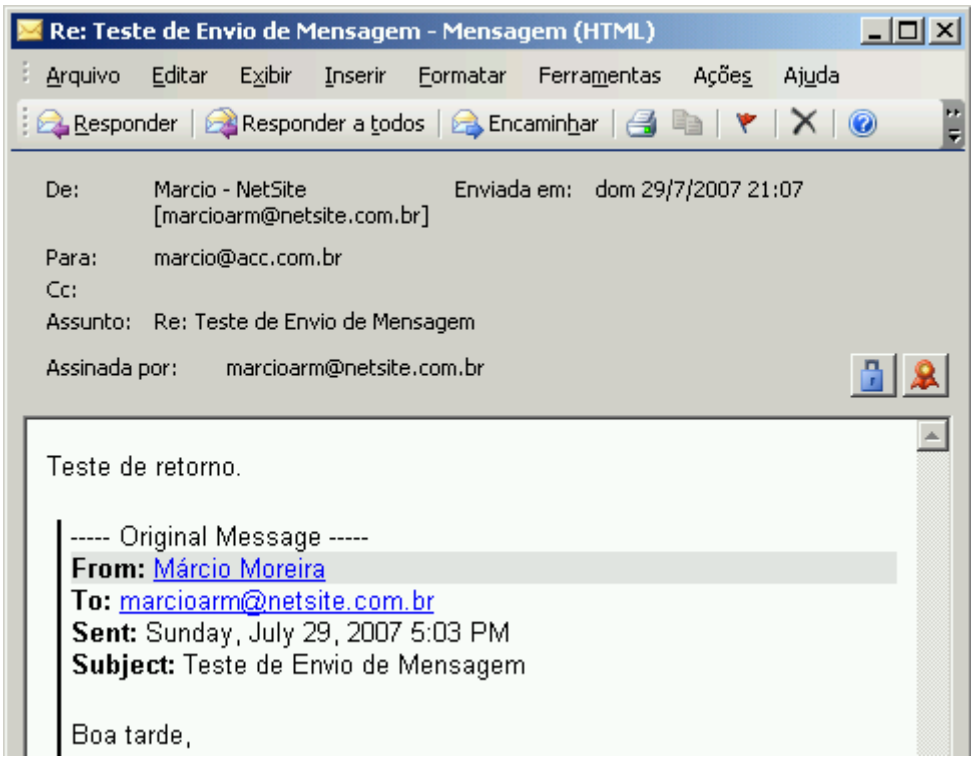

Figura 39 - Abrindo uma mensagem cifrada e assinada no Outlook.

5. O e-mail como prova

Neste capítulo é investigada a possibilidade de e-mails seguros, emitidos com certificados digitais gerados por autoridades certificadoras credenciadas, serem adotados como provas em questões jurídicas.

5.1. O documento eletrônico e a legislação

O documento eletrônico surgiu sob a forma de Lei no Decreto 3.714 de 03/01/2001, publicado no Diário Oficial da União (DOU) em 04/01/2001, que trata da remessa de informações por meio eletrônico. Mas, antes da entrada em vigor do novo código civil em 2003, o documento eletrônico tinha o mesmo valor de uma prova ou contrato verbal. O novo código civil em seus artigos 104 (princípio da liberdade de forma), 428 (contrato entre presentes) e 434 (contrato entre ausentes) regulou o comércio, inclusive o eletrônico, e viabilizou o documento eletrônico.

5.2. O certificado digital e os documentos eletrônicos

O certificado digital é citado pela primeira vez no Decreto 3.865 de 13/07/2001, que estabelece os requisitos para contratação de certificação digital pelos órgãos do governo federal. A Medida Provisória 2.200 de 24/08/2001 criou o ICP-Brasil (Infra-estrutura de chave pública do governo federal) com a responsabilidade de garantir autenticidade, integridade e validade jurídica de documentos eletrônicos. O Decreto 4.520 de 16/12/2002 definiu que documentos enviados ao DOU ou ao Diário da Justiça, para publicação, deveriam ser enviados somente sob a forma de documento eletrônico. Esse aparato normativo concedeu ao certificado digital a propriedade de garantir como prova o documento eletrônico que seja emitido por autoridade certificadora credenciada.

5.3. O uso do e-mail em questões jurídicas

Quanto à adoção do e-mail como prova jurídica, segundo Leitão Jr. [LEITÃOJR02] há duas correntes no Brasil. Uma que adota a admissibilidade direta e indireta e outra que se pauta pela admissibilidade direta e condicionada. Em ambos os casos a fragilidade do uso do e-mail como prova residia no fato deles não serem documentos assinados. Com o uso das

assinaturas digitais esta questão deve mudar, pois as assinaturas digitais garantem a autenticidade, integridade e o não repúdio da mensagem. Um bom resumo sobre esse assunto pode ser visto numa entrevista de Patrícia Peck, advogada especialista em direito digital, concedida à repórter Aline Pinheiro da revista Consultor Jurídico, publicada em 03/09/2006 sob o título "*A internet e a lei - Conteúdo que está no seu computador é público* "[PINHEIRO06].

Até 2004, como pode ser visto nos artigos "*Assinatura digital não é Assinatura formal*" de Angela Bittencourt Brasil de 2000 [BRASIL00], "*O documento eletrônico, a criptografia e o direito*" de Paulo Sá Elias de 2001 [ELIAS01] e "*O documento eletrônico na jurisprudência do Superior Tribunal de Justiça*" de Leonardo Netto Parentoni de 2004 [PARENTONI04], o Superior Tribunal de Justiça, e consequentemente o Judiciário Brasileiro, ainda não havia considerado o documento eletrônico, assinado digitalmente com um certificado digital, como uma forma legal e irrefutável de documento e consequentemente como prova. Nesses dois textos, nota-se claramente a movimentação da negação absoluta [BRASIL00] para uma negação relativa [ELIAS01] e [PARENTONI04], indicando a necessidade da legislação se adaptar à sociedade.

A Lei 11419 de 19 de dezembro de 2006, publicada no Diário Oficial da União em 20 de dezembro de 2006, que dispõe sobre a informatização do processo judicial, disponível em http://www010.dataprev.gov.br/sislex/paginas/42/2006/11419.htm (acessado em 29/7/2007). Esta lei em seu parágrafo 2º, inciso III, alínea a, reconhece como forma válida de assinatura eletrônica e identificação inequívoca do signatário: "*a) assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica*".

Mesmo antes da lei 11419, e-mails, inclusive não assinados digitalmente, já estavam sendo admitidos como provas em processos trabalhistas de demissão por justa causa e pagamento de horas extras. Exemplos de casos de demissão por justa causa podem ser vistos nos artigos "*E-mail causa demissão justa*" de Mariana Flores publicado no Correio Brasiliense de 17/05/2005 [FLORES05] e "*Mau uso de e-mail da empresa gera demissão por justa causa*" da Folha Online publicado em 10/07/2006 [FOLHAOL06]. O artigo da Mariana trás ainda que a 1ª Turma do TST (Tribunal Superior do Trabalho) considerou, já em 2005, que o e-mail corporativo não deve ser utilizado para fins pessoais e, portanto pode ser inspecionado para fins de prova em demissões por justa causa.

E-mails não assinados foram aceitos como prova para recebimento de horas extras num julgamento da 2ª Turma do TRT (Tribunal Regional do Trabalho) da 10ª Região, numa ação (Processo número 00279-2006-016-10-00-6-RO) entre um ex-empregado do Hotel Phenia Ltda, onde o magistrado relator (Brasilino Santos Ramos) cita na sentença: "*Entendo que a correspondência eletrônica, fruto do implemento da modernidade, constitui meio de prova, desde que não paire sobre ela nenhum indício de incorreção nos registros efetuados ou adulteração*". A decisão confirmou sentença de instância inferior.

Outro exemplo de admissibilidade de e-mails como provas é um Recurso Especial 566.468 (RJ 2003/0132555-7, disponível em www.cbeji.com.br/br/downloads/secao/jurispterra.pdf, acessado em 02/08/2007) da Terra Networks do Brasil S/A contra Iraci Monteiro de Carvalho, onde a Terra recorre ao STJ para não pagar uma indenização por danos morais reclamados por Iraci. Na ação proposta por Iraci, essa reclama que seu nome e telefone foram inclusos sem autorização em site de relacionamentos da Terra e por conta disto teve danos causados por e-mails disparados por clientes e usuários da Terra para ela. A 4ª Turma do STJ negou o recurso da Terra por decisão unânime. Esta decisão é um marco no judiciário brasileiro, tornando-se uma jurisprudência, pois além de responsabilizar a Terra por atitudes de seus clientes também representa a primeira condenação por danos morais por *spam* no Brasil.

Outra evidência da admissibilidade do certificado digital pode ser vista no julgamento de um Agravo de Instrumento 564765, julgado pelo STF (Supremo Tribunal Federal) em 14 de Fevereiro de 2006, publicado em 17 de março de 2006 no Diário da Justiça, disponível em www.stf.gov.br/jurisprudencia/nova/pesquisa.asp, acessado em 29/07/2007, onde foi relator o Ministro Supúlveda Pertence. Segue a ementa do julgamento reproduzida:

> Ato processual: recurso: chancela eletrônica: exigência de regulamentação do seu uso para resguardo da segurança jurídica. 1. Assente o entendimento do Supremo Tribunal de que apenas a petição em que o advogado tenha firmado originalmente sua assinatura tem validade reconhecida. Precedentes. 2. No caso dos autos, não se trata de certificado digital ou versão impressa de documento digital protegido por certificado digital; trata-se de mera chancela eletrônica sem qualquer regulamentação e cuja originalidade não é possível afirmar sem o auxílio de perícia técnica. 3. A necessidade de regulamentação para a utilização da assinatura digitalizada não é mero formalismo processual, mas, exigência razoável que visa impedir a prática de atos cuja responsabilização não seria possível. (grifo nosso).

Nesse caso a decisão, por maioria dos votos, foi por negar o agravo de instrumento. Como se pode ver nos precedentes, pelo uso de uma assinatura digital não chancelada pelo fato de não existir o certificado digital, emitido por autoridade certificadora credenciada, a assinatura digital torna-se uma mera chancela eletrônica sem valor jurídico até que se consiga uma perícia técnica. Por conta disto, o certificado digital, emitido por uma autoridade certificadora credenciada, na visão do STF, torna a assinatura digital válida como forma de responsabilização inequívoca do autor, independentemente de perícia técnica.

Logo, o e-mail que utiliza uma assinatura digital gerada por certificado digital emitido por uma Autoridade Certificadora Credenciada, atende aos requisitos de identificação inequívoca e tem o valor de uma assinatura do signatário. Não havendo, portanto, razões para não se admitir o uso de e-mails assinados como provas em questões judiciais.

6. Conclusão

Com relação à hipótese de que deve existir um protocolo que permita o uso de e-mails seguros, conforme demonstrado no laboratório realizado e descrito no capítulo 3, o S/MIME é um protocolo padrão de mercado que atende aos requisitos de segurança propostos (confidencialidade, autenticidade e integridade). Logo, o S/MIME comprova esta hipótese. O S/MIME também apresenta o benefício de ser um protocolo fim a fim. Isto quer dizer que somente os MUA precisam suportar esse protocolo, pois ele é transparente para os demais agentes de e-mail envolvidos. Portanto, os provedores de serviços de e-mail precisam disponibilizar apenas o suporte ao protocolo MIME que é utilizado pelo S/MIME.

No capítulo 3 também foram analisados os protocolos SMTP, POP3, IMAP, SPF e DKIM. Também conforme demonstrado, todos esses protocolos não atendem aos requisitos de segurança propostos para os e-mails seguros. No caso do SPF não há assinatura digital nem garantia de integridade e confidencialidade da mensagem, mas a rejeição de mensagens cuja origem não possa ser comprovada é muito útil. No caso do DKIM, fora da região assinada a mensagem pode ser interceptada e alterada facilmente, mas idéia do provedor do emissor ser co-responsável pelo envio da mensagem vai de encontro à visão da justiça.

O SPF e o DKIM são demonstrações claras da indignação dos provedores de serviço e dos fabricantes de softwares de e-mails com os *spams*. Entretanto, como a adoção do S/MIME para redução dos *spams* depende dos usuários, para ativação de filtros em seus MUAs, ou dos provedores de serviços para reduzir o tráfego de mensagens cujas origens não possam ser comprovadas ou ainda para disponibilizar regras de eliminação de *spams* antes de chegarem no MUA do usuário destino. Acredita-se que o SPF e o DKIM, ou pelo menos seus princípios, se somarão ao S/MIME na batalha contra os *spams*.

Como já existe um protocolo que atende aos requisitos de segurança propostos, não foi necessário a definição e implementação de um novo protocolo. Por conta disto, o capítulo 4 foi dedicado à descrição de como utilizar adequadamente o protocolo S/MIME. A divulgação deste trabalho e o início da utilização de e-mails seguros por parte daqueles que tiverem acesso a ele contribuirá para acelerar o processo de redução dos *spams*.

Outra hipótese comprovada no capítulo 5, foi a de que os e-mails seguros, emitidos com certificados digitais gerados por autoridades certificadoras credenciadas, podem ser utilizados como provas em questões jurídicas. Mostrou-se que mesmo e-mails não assinados digitalmente estão sendo utilizados como provas em demissões por justa causa e em ações de danos morais. Nesta última questão revelou-se uma decisão que se tornou jurisprudência, onde um provedor de serviços foi condenado pela emissão de *spams* de um de seus clientes.

Para minimização dos *spams* com o S/MIME, os usuários, as organizações e os provedores de serviços de e-mail podem contribuir. Os usuários podem assinar digitalmente suas mensagens e incluir filtros eliminando ou movendo mensagens não assinadas para pastas de avaliação. As organizações podem adotar políticas exigindo que as mensagens emitidas por seus membros sejam assinadas digitalmente e rejeitando mensagens não assinadas ou cujo endereço de retorno não possa ser comprovado. Os provedores também podem adotar políticas que obriguem as mensagens emitidas em seus domínios terem o endereço de retorno corretamente definidos, disponibilizando configurações para que os usuários ou organizações rejeitem ou tratem mensagens não assinadas ou cujo endereço de retorno não possa ser comprovado, bem como configurando adequadamente seus serviços para que *spammers* não possam explorá-los. Para que o S/MIME gere os benefícios esperados pelo menos um desses grupos (usuários, organizações ou provedores) precisa adotar as medidas sugeridas. Naturalmente, o melhor resultado será conseguido se todos esses grupos adotarem as medidas sugeridas.

As recomendações e sugestões deste trabalho não invalidam as iniciativas já empreendidas para minimização dos *spams*, tais como: *black lists, white lists, gray lists*, mudança da porta de envio de e-mail, softwares *anti-spam*, *honeypots*, etc. Pelo contrário, essas iniciativas foram essenciais para que o quadro não fosse pior do que o atual. Além disto, muitas delas continuarão sendo úteis por muito tempo. Acredita-se que as sugestões e recomendações desse trabalho se somarão a essas iniciativas no combate aos *spams* e aos *spammers*. Caberá a cada administrador de serviços (dos prestadores de serviços de e-mail) ou de sistemas (das organizações) escolher as sugestões, recomendações e iniciativas que sejam mais adequadas às suas necessidades.

Por outro lado, como os recursos de infra-estrutura de software, necessários para a adoção das recomendações e sugestões deste trabalho já estão disponíveis ou estão em fase de disponibilização, acredita-se que o custo para a adoção de tais medidas seja baixo, pois estará muito mais relacionado à definição e implementação das políticas recomendadas do

que em investimentos e custos operacionais relacionados à infra-estrutura. A mudança está mais relacionada a questões culturais (cultura de organizações) do que a fatores econômicos. Por esta razão, acredita-se que a adoção de tais sugestões e recomendações será gradual, progressiva e irreversível. Logo, cada usuário, administrador de sistemas ou de serviços poderá dar sua contribuição neste processo assinando digitalmente seus e-mails e adotando políticas neste sentido.

Diante do exposto, conclui-se que como a adoção dos e-mails seguros é simples e transparente para os provedores de serviço. Acredita-se que as empresas e posteriormente as pessoas adotarão esse tipo de e-mail. Os provedores de serviços de e-mails, para evitar ações judiciais, passarão a evitar a emissão de *spams* em seus domínios. Logo, e-mails cuja origem seja desconhecida ou não possa ser comprovada passarão a ser rejeitados por toda a comunidade da Internet. Como os *spammers* poderão ser responsabilizados por seus atos, consequentemente eles reduzirão significativamente a emissão de *spams*.

6.1. Trabalhos futuros

A presente pesquisa pode ser estendida para:

- Analisar a interoperabilidade dos certificados digitais, do mesmo padrão (por exemplo, X.509), emitidos por autoridades certificadoras diferentes, sejam elas credenciadas ou não.
- Detalhar a utilização do S/MIME para outros MUA, tais como: Outlook Express e Lotus Notes.
- Estudar a implantação de PKI (infra-estrutura de chave pública) para uma organização considerando o uso de certificados digitais para trocas de e-mails.
- Analisar estratégias de acelerar a adoção de e-mails seguros pela comunidade da Internet.

7. Referências

[ANTISPAM06] Comitê Gestor da Internet no Brasil. *Problemas causados pelo spam*. 2006. Disponível em: www.antispam.br/problemas/. Acessado em: 20/07/2006.

[BAILEY04] BAILEY, David. *Utilizing Open-Source Software to Build a (Relatively) Secure, Spam- and Virus-Free Mail Service*. 2004. Disponível em: www.sans.org/reading_room/whitepapers/email/1402.php. Acessado em: 20/07/2006.

[BRADEN89] BRADEN, R. *Requirements for Internet Hosts - Application and Support*. RFC 1123. IETF. 1989. Disponível em: http://tools.ietf.org/html/rfc1123. Acessado em: 30/04/2007.

[BRASIL00] BRASIL, A. *Assinatura digital não é Assinatura formal*. CBEJI. 2000. Disponível em: www.cbeji.com.br/artigos/artang02.htm. Acessado em: 29/07/2007.

[CHAU05] CHAU, David. *Prototyping a Lightweight Trust Architecture to Fight Phishing*. MIT. 2005. Disponível em: http://theory.lcs.mit.edu/~cis/theses/chau-uap.pdf. Acessado em: 02/05/2007.

[CRISPIN03] CRISPIN, M. *Internet Message Access Protocol - Version 4rev1*. RFC 3501. IETF. 2003. Disponível em: http://tools.ietf.org/html/rfc3501. Acessado em: 01/05/2007.

[DELANY07] ALLMAN, E., CALLAS, J., DELANY, M., FENTON, J. and THOMAS, M. *DomainKeys Identified Mail (DKIM) Signatures*. RFC 4871. IETF. 2007. Disponível em: www.ietf.org/rfc/rfc4871.txt. Acessado em: 30/05/2007.

[ELIAS01] ELIAS, P. S. *O documento eletrônico, a criptografia e o direito*. Jus Navigandi. 2001. Acessado em 30/07/2007. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=2073.

[FLORES05] FLORES, M. *E-mail causa demissão justa*. Correio Brasiliense. Justiça. 2005. Disponível em: www.serpro.gov.br/noticiasSERPRO/20050517_05. Acessado em: 02/08/2007.

[FOLHAOL06] Folha Online. *Mau uso de e-mail da empresa gera demissão por justa causa*. Folha de São Paulo. 2006. Acessado em 02/08/2007. Disponível em: http://www1.folha.uol.com.br/folha/informatica/ult124u20327.shtml.

[FTC98] Federal Trade Comission. *FTC Names Its Dirty Dozen:12 Scams Most Likely to Arrive Via Bulk E-mail*. FTC. Jully 1998. Acessado em: 21/04/2007. Disponível em: www.ftc.gov/bcp/conline/pubs/alerts/doznalrt.shtm.

[FUSCO05] FUSCO, Camila. *Certificação digital: você já tem a sua?*. IDG Now. 2005. Disponível em: http://www.serpro.gov.br/noticiasSERPRO/20050804_03. Acessado em: 25/07/2007.

[GARFINKEL05] GARFINKEL, Simson; MARGRAVE, David; SCHILLER, Jeffrey; et al. *How to Make Secure E-mail Easier To Use*. 2005. Disponível em: http://people.csail.mit.edu/rcm/chi_smime.pdf. Acessado em: 20/07/2006.

[GOMES06] GOMES, Wagner. *Envio de spam disparou em janeiro e passou de 286 mil mensagens no país*. Globo Online. 2006. Disponível em: http://oglobo.globo.com/online/tecnologia/plantao/2006/02/14/191850174.asp. Acessado em: 17/07/2006.

[HAMBRIDGE99] HAMBRIDGE, S. *A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)*. RFC 2635. IETF. 1999. Disponível em: www.ietf.org/rfc/rfc2635.txt. Acessado em: 15/04/2007.

[HOFFMAN04] HOFFMAN, Paul. *S/MIME and OpenPGP*. Internet Mail Consortium. 2004. Disponível em: www.imc.org/smime-pgpmime.html. Acessado: 02/05/2007.

[ITI05] ITI. *O que é cerificação digital?* Instituto Nacional de Tecnologia da Informação. 2005. Acessado em: 25/07/2007. Disponível em: www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf.

[JANUARIO07] JANUÁRIO, Larissa. *Tutorial parte II: O que fazer com um certificado digital*. WnNews. 2007. Disponível em: http://wnews.uol.com.br/site/noticias/materia_especial.php?id_secao=17&id_conteudo=418. Acessado em: 25/07/2007.

[KLENSIN01] KLENSIN, J. *Simple Mail Transfer Protocol*. RFC 2821. IETF. 2001. Disponível em: http://tools.ietf.org/html/rfc2821. Acessado em: 30/04/2007.

[LEITÃOJR02] LEITÃO JR., Esdras. *O e-mail como prova no Direito*. Jus Navigandi. 2002. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=3025. Acessado em: 18/07/2006.

[M&ROSE96] MYERS, J. and ROSE, M. *Post Office Protocol - Version 3*. RFC 1939. IETF. 1996. Disponível em: http://tools.ietf.org/html/rfc1939. Acessado em: 30/04/2007.

[MARCEL06] MARCEL F. Souza. *Segurança em Servidores de Correio Eletrônico*. Uniminas. 2006. Disponível em: www.si.uniminas.br/TFC/monografias/. Acessado em: 15/04/2007.

[MODULO02] Módulo Security Magazine. *Pesquisa revela que spam causa 10% de perda de tempo em empresas*. Módulo. 29/07/2002. Acessado em: 30/09/2007. Disponível em: www.modulo.com.br/index.jsp?page=3&catid=7&objid=1251.

[MSGLABS06] MessageLabs. *Threat Statistics - Spam*. 2007. Disponível em: www.messagelabs.com/StatisticsThreat/StatisticsThreatType=Spam. Acessado em: 21/04/2007.

[NGSS06] Next Generation Security Software. *The Phishing Guide Understanding and Preventing Phishing Attacks*. NISCC. 2006. Disponível em: www.lions.org.uk/PDF/phishing_guide.pdf. Acessado em: 02/05/2007.

[PARENTONI04] PARENTONI, L. *O documento eletrônico na jurisprudência do Superior Tribunal de Justiça*. 2004. Jus Navigandi. UOL. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=6099. Acessado em: 29/07/2007.

[PATELCJ01] PATEL, V., CHANDRA, A. and JAIN, S. *Electronics mail security (PGP & S/MIME)*. 2001. George Mason University. Acessado em: 02/05/2007. Disponível em: http://ise.gmu.edu/~eschneid/infs612/projects/email_sec.pdf.

[PINHEIRO06] PINHEIRO, Aline. *A internet e a lei - Conteúdo que está no seu computador é público*. Entrevista de Patrícia Peck à revista Consultor Jurídico de 3/9/2006. Disponível em: http://www.fraudes.org/clipread.asp?CdClip=614. Acessado em: 10/08/2007.

[POSTEL82] POSTEL, Jonathan B. *Simple Mail Transfer Protocol*. RFC 821. IETF. 1982. Disponível em: http://tools.ietf.org/html/rfc821. Acessado em: 30/04/2007.

[R&KORVER03] RESCORLA, E. and KORVER, B. *Guidelines for Writing RFC Text on Security Considerations*. RFC 3552. IETF. 2003. Disponível em: www.ietf.org/rfc/rfc3552.txt. Acessado em: 02/05/2007.

[RAMOS&A04] RAMOS, G., SIQUEIRA, T., CANSIAN, A. e CANDIDO Jr, A. *Análise de Desempenho de Políticas de Segurança em Servidores de Correio Eletrônico*. I2TS. Acm Security. 2004. Disponível em: www.acmesecurity.org/publicacoes/artigos/acme-paper-i2ts-2004-gus-thi-arn-adr.pdf/download. Acessado em: 28/07/2007.

[RAMSDELL04] RAMSDELL, B. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*. RFC 3851. IETF. 2004. Disponível em: www.ietf.org/rfc/rfc3851.txt. Acessado em: 01/05/2007.

[SETAPA01] SETAPA, Sharipah. *Securing E-Mail*. 2001. Disponível em: www.niser.org.my/resources/secure_email.pdf. Acessado em: 20/07/2006.

[SOUZA06] SOUZA, M. *Segurança em Servidores de Correio Eletrônico*. Uniminas. 2006. Disponível em: www.si.uniminas.br/TFC/monografias/marcel_mono_Pos46.pdf. Acessado em: 02/05/2007.

[STALLINGS99] STALLINGS, W. *Cryptography and Network Security: Principles and Practice*, Prentice Hall, 1999.

[VERISSIMO03] VERISSIMO, *Fernando. SPAM: Levantando uma discussão*. Academia Brasileira de Ciências. 2003. Acessado em 30/09/2007. Disponível em: www.abc.org.br/~verissimo/textos/spam.pdf.

[WONG&S06] WONG, M. and SCHLITT, W. *Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1*. RFC 4408. IETF. 2006. Disponível em: www.ietf.org/rfc/rfc4408.txt. Acessado em: 30/05/2007.