Centro Universitário de Brasília

Instituto CEUB de Pesquisa e Desenvolvimento – ICPD

HEWDON LUCCAS TAVARES COSTA

PROPOSTA DE SOLUÇÃO PARA A AUDITORIA EM MENSAGENS CRIPTOGRAFADAS UTILIZANDO HSM

Brasília

2016

HEWDON LUCCAS TAVARES COSTA

PROPOSTA DE SOLUÇÃO PARA A AUDITORIA EM MENSAGENS CRIPTOGRAFADAS UTILIZANDO HSM

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu*, na área Redes de Computadores com Ênfase em Segurança.

Orientador: Mestre Gilberto de Oliveira Netto

Brasília, ___ de _____ de ____.

Banca Examinadora

_____

Prof. Dr.

_____

Prof. Dr.

_____

Prof. Dr.

AGRADECIMENTO

Primeiramente, gostaria de agradecer a Deus, por ser a essência de minha vida, por me dar força e coragem nos dias de luta, e não me deixar desamparado nos momentos de aflição, a Ele toda honra e glória.

Agradeço especialmente também a minha amada esposa, por sua compreensão, zelo e carinho que tem para comigo, sendo a cada dia uma incrível companheira, me ajudando e me acompanhando nos momentos de alegria e tristeza.

Por fim, agradeço aos meus familiares e ao meu professor-orientador, por a cada dia me passar mais confiança e incentivo nesta grande caminhada ao conhecimento.

RESUMO

Com a crescente utilização e importância do correio eletrônico no âmbito mundial, organizações públicas e privadas se mostram preocupadas com o sigilo e a integridade dos dados que perpassam neste sistema, com isso, mecanismos de segurança para proteger esta comunicação tem se desenvolvido constantemente. Como exemplo, pode-se citar a utilização dos recursos das criptografias simétrica e assimétrica. Resolvido o problema do sigilo e da integridade, como garantir a auditabilidade dessas informações criptografadas? Como garantir que o próprio usuário, ao perder sua chave para cifrar uma mensagem, consiga ter aceso a esta mensagem? Este trabalho propõe uma solução de auditoria de quebra de sigilo composta por procedimentos e recursos tecnológicos como o HSM (Hardware Security Module ou Módulo de Segurança Criptográfico) que permite a descriptografia segura de uma mensagem cifrada.

Palavras-chave: correio eletrônico governamental, criptografia simétrica e assimétrica, HSM (Hardware Security Module), auditoria e e-mail criptografado.

ABSTRACT

With the increasing use and importance of e-mail at the global, public and private organizations show concerned with the confidentiality and integrity of the data that underlie this system with this security mechanisms to protect this communication has developed constantly. As an example, we can mention the use of resources of symmetric and asymetric encryptions. Solved the problem of confidentiality and integrity, and ensure the auditability of the information encypted? Hom to ensure that the user himself, to lose your key to encrypt a message, can be lit to this message? This paper proposes a breach of confidentiality of audit solution composed of procedures and technological resources such as HSM (Hardware Security Module Cryptographic or Security Module) that allows secure decryption of an encrypted message.

Keywords: government e-mail, symmetric and asymetric encryption, HSM (Hardware Security Module), auditing and encrypted email

SUMÁRIO

1. INTRODUÇÃO

Com a crescente disseminação da Internet em nível mundial, e com a necessidade cada vez mais incessante em se utilizar ferramentas de comunicação eletrônica, tais como correio eletrônico, é imprescindível que se aplique para tanto, mecanismos de proteção para que esta comunicação, seja privada e segura, a ponto de que mesmo se houver interceptação, o atacante não consiga visualizar o conteúdo da mensagem.

No âmbito do Governo Federal Brasileiro, o decreto presidencial 8.135 de 04 de novembro de 2013 no § 3º determina que *"os programas e equipamentos deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações".*

Com base também no decreto, pode-se afirmar que o correio eletrônico utilizado no Governo Federal como sendo uma ferramenta oficial de comunicação, tem que possuir mecanismos que assegurem tais características e que possa ser passível de se realizar auditoria, que se entende neste trabalho por quebra de sigilo das informações, nos casos em que haja necessidade.

Sabe-se que a confidencialidade é a propriedade da informação na qual esta não estará disponível ou divulgada às pessoas não autorizadas. E autenticidade, é a propriedade na qual se assegura que quem originou a informação é de fato quem diz ser. Já disponibilidade, é a característica que a informação tem que estar acessível a quem de direito é, a qualquer tempo. E integridade, por sua vez é a capacidade que a informação tem para garantir que seu conteúdo está íntegro e não foi modificado ao longo da transmissão.

Logo, para que estas características específicas da qual o decreto presidencial determina, sejam aplicadas dentro do sistema de correio eletrônico, ou

seja, para se garantir que uma mensagem (e-mail) tenha em sua essência tanto a confidencialidade quanto a autenticidade, é que a criptografia deve se fazer presente, além disso, os outros princípios também são essenciais para este sistema, pois terá que ser disponível a todos dos quais fazem uso, bem como garantir formas de que a mensagem criada não seja alterada no decorrer de sua transmissão, ou até mesmo no seu armazenamento.

Contudo, estas afirmações só tem sentido completo, se for aplicado também na visão de que caso um e-mail gerado em modo criptografado, possa também ser auditado, ou seja, que sua quebra de sigilo possa ser executada, mesmo que não se tenha as chaves privadas dos participantes da comunicação a fim de realizar a descriptografia da mensagem.

Então, como fazer para caso tenha a necessidade de auditar ou analisar esta informação que ora fora criptografada, e que somente os envolvidos nessa comunicação é que tem a chave para descriptografá-la?

Como forma de solução deste problema, o estudo se propõe a demonstrar a integração do Módulo de Hardware Criptográfico (HSM) com o correio eletrônico, criando uma solução de auditoria de quebra de sigilo segura e confiável.

No intuito de facilitar a melhor compreensão, o estudo está dividido em objetivos específicos que fornecem uma estrutura lógica e funcional de como pode ser realizada esta solução.

Incluindo esta introdução, a monografia estrutura-se da seguinte forma:

O capítulo 2 apresenta os pré-requisitos, traçando o objetivo, mostrando a metodologia e apresentando as justificativas do trabalho

O capítulo 3 é composto pelo referencial teórico, em que se subdivide em 5 tópicos, são eles:

Auditoria: demostrado através de um detalhamento teórico de conceituação, origem e importância no meio da sociedade, focando na área tecnológica, fornecendo subsídios aos outros tópicos.

Correio eletrônico: detalhamento conceitual, histórico e tecnológico deste sistema, sendo um dos pontos focais deste trabalho.

Criptografia: explicação técnica e conceitual, mostrando as benesses de se implementar os mecanismos oriundos da criptografia no cenário tecnológico de troca de informações, tendo em vista o aspecto global da internet.

ICP Brasil: conceituação de forma bem didática e organizada, de que como é formada e qual sua importância para a certificação digital.

HSM: explicação técnica e conceitual detalhada, mostrando seus recursos e aplicabilidade ao cenário proposto no decorrer deste trabalho.

O capítulo 4 traz a solução de auditoria proposta, se concentrando então no desenvolvimento deste trabalho, sendo subdividido em 3 tópicos, são eles:

A solução: após a explanação do problema, é mostrado de modo didático e objetivo, a proposta de solução adotada, bem como os processos que foram desenvolvidos para torná-la factível, possibilitando a sua aplicabilidade em qualquer organização, que assim a queira.

Integração do HSM com correio eletrônico: detalha os procedimentos técnicos necessários a realização desta integração entre o hardware criptográfico HSM e o sistema de correio eletrônico.

Executando a auditoria: detalhamento procedimental de como é realizado o processo de auditoria, através da solução que fora proposta, dando um completo entendimento acerca do tema deste trabalho.

O capítulo 5 apresenta a conclusão, onde são mostrados os resultados

adquiridos com a solução, servindo também como base de conhecimento para que novos trabalhos sejam desenvolvidos através do tema proposto.

2. REQUISITOS PRÉ PESQUISA

OBJETIVO

Este estudo tem como objetivo principal, apresentar uma solução que forneça os meios necessários para efetuar a quebra de sigilo em mensagens criptografadas.

Para isto, será abordada a importância da criptografia na segurança da informação e das comunicações, voltado especificamente para o cenário de correio eletrônico, bem como os recursos tecnológicos hoje disponíveis para que se possa realizar tal objetivo, fazendo então um elo entre estes.

Vale salientar que o correio eletrônico utilizado nesta monografia, é adotado no âmbito do Governo Federal, logo, todos os processos mostrados e definidos podem se aplicados em sua totalidade dentro de qualquer instituição governamental, como também, não há impeditivo nenhum para que sua aplicabilidade tenha sucesso dentro de uma organização privada.

JUSTIFICATIVA

Entende-se que as informações geradas através do serviço de correio eletrônico provido por uma instituição seja ela governamental ou privada, são de propriedade desta instituição, mesmo que seus colaboradores sejam os responsáveis por criá-las.

Partindo desse pressuposto, e também da necessidade de que hoje, as trocas de informações exijam um nível de segurança para que os dados contidos nelas não sejam interceptados ou até mesmos decifrados – neste caso utilizando processo de criptografia e descriptografia – as organizações têm se preocupado cotidianamente com o sigilo das informações.

Para garantir então esta segurança, o serviço de correio eletrônico governamental, tem implantado a funcionalidade de criptografia, com o intuito de prover total confidencialidade e integridade nas trocas de informações, utilizando chaves privadas individuais, de conhecimento exclusivo dos mesmos.

Logo, a organização precisa possuir mecanismos de realizar a quebra de sigilo mesmo em e-mails que foram criptografados, partindo para tanto, do pressuposto, que não necessitará das chaves privadas dos participantes da comunicação para realizar tal necessidade.

METODOLOGIA

A presente proposta de solução de auditoria foi realizada durante todo o ano de 2015 na empresa pública do governo federal, na qual possui um correio eletrônico implementado para seus empregados e que, recentemente liberou a funcionalidade de criptografia de suas mensagens aos seus usuários.

É resultado então da experiência prática real, com a solução implementada nesta instituição e em operação desde então.

Com o objetivo de atingir o que o trabalho se propõe a executar, deverá ser seguido cada objetivo específico de forma sequencial.

Com isso a estrutura de conhecimento e entendimento será melhor compreendida e aplicada.

Serão identificadas cada forma possível de requisição legal para se executar a auditoria.

Haverá a descrição detalhada do funcionamento do hardware criptográfico e sua forma de integração com o correio eletrônico, a fim de propiciar a execução da quebra de sigilo.

3. REFERENCIAL TEÓRICO

3.1 AUDITORIA

Com base no crescimento que as organizações vêm tendo, e em paralelo com a evolução bastante acelerada da tecnologia, fez com que as atividades manuais se tornassem automatizadas. Com isso, o ambiente de negócios tem se tornado cada vez mais complexo e desafiador para os gestores das empresas de praticamente qualquer mercado e, consequentemente, as áreas produtivas e administrativas foram se automatizando por sistemas e ambientes de tecnologia da informação.

Tais ambientes tecnológicos são responsáveis pelo processamento e armazenamento de um dos bens mais valiosos dentro de uma organização: a informação.

Diante deste contexto, o investimento em segurança da informação se torna vital para que uma empresa não esteja exposta a riscos.

Logo, se faz necessário que medidas de controle e segurança de sistemas sejam revisadas e avaliadas sistematicamente por auditores, a fim de assegurar a proteção dos bens e serviços existentes em todas as áreas da empresa.

Sendo assim, a auditoria de sistemas se propõe a analisar os recursos computacionais (físicos e/ou lógicos), processos e pessoas dentro de uma organização, realizando isto, através da avaliação e da adequação das tecnologias, controles e sistemas de informação utilizados.

Identificadas falhas, erros, irregularidades ou ineficiência nestes controles, cabe a auditoria fazer recomendações em seu parecer, para correção e melhoria com o intuito de minimizar os riscos encontrados.

O princípio da auditoria se dá então, no fato de que é importante para uma organização, validar os processos aplicados em todas as suas áreas.

O seu surgimento se deu no século XVIII na Inglaterra, decorrente do crescimento das atividades industriais e da necessidade de resolver problemas contábeis originados das fraudes e erros que estavam ocorrendo.

Após anos, com o capitalismo em ascensão, a profissão de contador tornou-se mais reconhecida e difundida. Logo, em 1934 após a criação da Exchange Security Commission, nos Estados Unidos, uma nova profissão surge, a de auditor, em que esta ganhou novo estímulo e relevância no mercado.

Já no Brasil, a auditoria foi oficialmente organizada em 1957 a partir da formação do Instituto Público de Contadores do Brasil impulsionada pela expansão das atividades econômicas, associadas ao número de empresas estrangeiras que começaram a se instalar no país.

Segundo o escritor e auditor contábil, "*auditar é examinar, a fim de encontrar evidências de que o objeto em questão foi ou não executado"*. (ATTIE, 2000, p.36)

De modo geral, auditoria pode ser definida como uma atividade de exame e avaliação de procedimentos, processos, sistemas, registros e documentos com o objetivo de aferir o cumprimento dos planos, metas, objetivos e políticas da organização.

Segundo o dicionário Aurélio, auditoria é "o exame analítico e pericial que segue o desenvolvimento das operações contábeis desde o início até o balanço".

Logo, a auditoria se divide em dois tipos:

- Auditoria Interna ou Operacional: é aquela em que o auditor é funcionário da empresa e a revisão das atividades é contínua.

- Auditoria Externa ou Independente: é aquela em que o auditor pertence a uma empresa terceira e independente, e o exame das informações comprobatórias das demonstrações auditadas são periódicas, geralmente semestral ou anual.

Muito embora existam dois tipos de auditoria, o trabalho executado tanto pela interna, quanto pela externa é o mesmo. Ambas executam seu trabalho seguindo técnicas de auditoria, fazendo avaliações dos controles da organização e formulando sugestões de melhorias para as falhas encontradas.

Como mencionado na introdução deste trabalho, auditoria se dá também na forma de quebra de sigilo da informação.

E esta forma de auditoria se relaciona com a forma em que o escritor e auditor contábil *Attie* descreveu acima, pois para que se examine um objeto, e aqui entende-se por uma informação que esteja criptografada, é necessário que se busque evidências, ou seja, através de um processo de descriptografia na qual o resultado será um texto em forma legível, em que servirá de base para sustentar através de requisições legais aquilo que esteja investigando ou apurando.

A quebra de sigilo no aspecto da legislação brasileira, se fundamenta na necessidade de que em uma investigação civil contra agente público, sendo este pessoa física ou jurídica, mediante autorização judicial, possa apurar ato ímprobo, ou seja, situação em que não se encontram elementos suficientes para embasar uma Ação Civil Pública por ato que decorra de prejuízo ao erário, enriquecimento ilícito, ou infração a princípios constitucionais ou administrativos.

3.2 SISTEMA DE CORREIO ELETRÔNICO

O correio eletrônico é uma das aplicações da Internet mais difundidas, devido à sua facilidade de uso, e ao amplo poder de troca de informações, que permite através de uma simples troca de mensagens, enviar textos, transferir programas, fotos, planilhas, ou qualquer outro arquivo, sendo considerado uma inovação e evolução no modelo de comunicação mundial.

A origem da troca de informações por meio eletrônico se iniciou em 1844, com a criação do Código Morse, realizado por Samuel B. Morse, que consistia na transmissão de mensagens através de pontos e traços, correspondendo estes, a impulsos elétricos que como resultado emitia sinais acústicos ou luminosos com um certo intervalo de tempo, através de eletroímãs, podendo ser captadas por diversos aparelhos, como o radiotelégrafo e o telégrafo.

A figura 1 mostra o formato dos códigos utilizados para a transmissão.

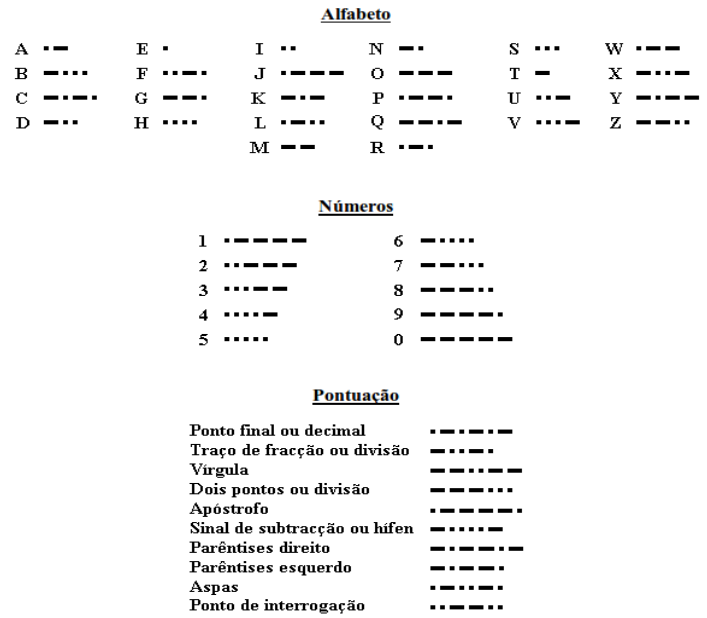

Figura 1: Alfabeto Código Morse

Desde então, a comunicação vem se evoluindo, a ponto de que em sistema de troca de mensagens entre computadores, o AUTODIN *(Automatic Digital Network), que* em português significa Rede Digital Automática, foi o pioneiro, sendo criado em 1966.

Este sistema foi desenvolvido para apoiar as comunicações militares dos Estados Unidos da América.

Logo, a ARPANET que é uma Agência de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos em 1969 aumentou significativamente a popularidade do correio eletrônico, originando a primeira rede operacional de computadores à base de comutação de pacotes.

Já em 1971, o programador Roy Tomlison iniciou o uso do sinal "@" para separar os nomes de usuário e da máquina, possibilitando com isso o envio correto entre sistemas diferentes de correio eletrônico.

A evolução deste sistema é crescente, e hoje em dia, pode-se afirmar que a utilização do correio eletrônico é essencial para a comunicação.

Este sistema é composto de dois subsistemas, um referente ao agente de usuário – responsável pela leitura e envio das mensagens –, e outro por agente de transporte – responsável pela transferência da mensagem –, sob estes agentes se encontram os protocolos de comunicação, que são encarregados por levar a mensagem entre um remetente a um ou vários destinatários de maneira rápida e segura.

O funcionamento do sistema para troca de mensagens ocorre da seguinte maneira: Um usuário que queira enviar uma mensagem para outro, utiliza um aplicativo de correio eletrônico, também conhecido como MUA *(Mail User Agent)* ou Agente de Mensagens do Usuário. Uma vez redigida a mensagem, esta é enviada

pelo MUA a um MTA *(Mail Transport Agent)*, Agente Transportador de Mensagens, que se encarrega então de entregar ao MTA do destinatário, este por sua vez, envia a mensagem para seu respectivo MUA, que coloca então a mensagem na caixa postal do destinatário.

A transferência da mensagem entre o MUA e o MTA utiliza o protocolo chamado SMTP *(Simple Mail Transfer Protocol)*, em português, Protocolo Simples de Transferência de Mensagens que está preconizado na RFC 5321.

Apenas para entendimento, RFC (*Request For Comments)*, é um conjunto de documentos que descrevem, especificam e parametrizam a respeito de normas, tecnologias e protocolos ligados à Internet.

O protocolo SMTP também se dá na comunicação entre o MTA do remetente e o MTA do destinatário, atuando na porta 25 e/ou 465 do TCP *(Transmission Control Protocol)* ou Protocolo de Controle de Transmissão, se utilizar para isso a camada de segurança conhecida como SSL *(Secure Socket Layer)*, ou seja, Camada de Canal Segura, que tem por objetivo estabelecer um canal criptografado entre um navegador (*browser*) a um sistema de Internet para que os dados trocados entre estes sejam protegidos.

A figura 2 ilustra como o servidor SMTP envia mensagem ao outro. No passo 1(um) o servidor emissor da mensagem através do comando *Helo ou Hello* informa o seu nome para que o servidor destinatário possa reconhecê-lo e aceitar a conexão, no passo 2(dois) o comando *MAIL From* inicializa a transação de e-mail informando quem será o remetente da mensagem, no passo 3(três) o comando *RCPT To* informará ao servidor destino quem será(ão) o(s) destinatário(s), já nos passos 4 e 5 (quatro e cinco) são enviadas a(s) mensagem(s) e ao final do conteúdo será colocado um .(ponto) em uma linha vazia significando que toda a mensagem foi

enviada, no último passo o 6(seis) o servidor destinatário responderá ao SMTP emissor que a conexão será fechada.

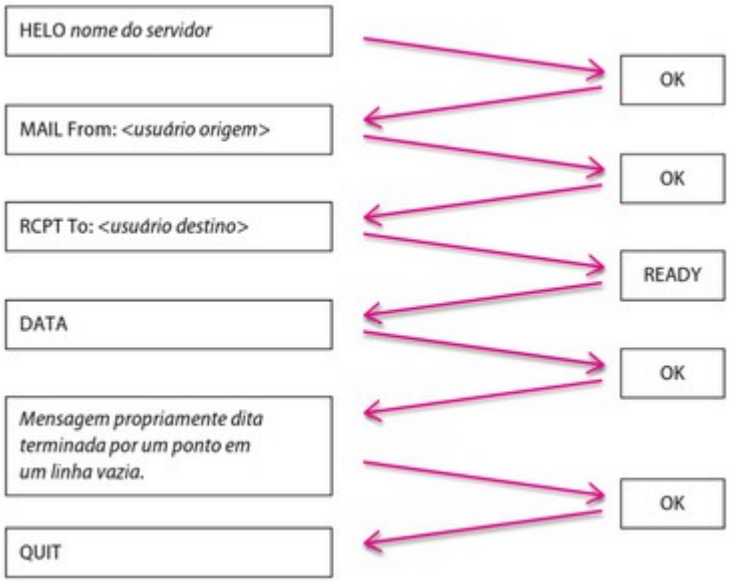

Figura 2: Início da comunicação via SMTP

É importante notar que este processo é executado toda vez que for enviar alguma mensagem.

O servidor de correio eletrônico do destinatário, quando receber uma mensagem para um dos seus usuários, simplesmente a colocará na caixa postal referente. A transferência de mensagens recebidas entre o servidor e o cliente de correio eletrônico requer a utilização de outros programas e protocolos.

O protocolo POP (Post Office Protocol), Protocolo de "Agência" de Correio, firmado pela RFC 1939, pode ser utilizado para este fim, pois guarda as mensagens dos usuários em caixas postais, e aguarda até que estas sejam acessadas.

Observa-se que neste protocolo, ao se ler as mensagens, estas serão copiadas para o computador local. A porta original de utilização do POP é a 110 do TCP, podendo ser 995 se utilizar em conjunto com o SSL.

A figura 3 descreve como se dá a requisição utilizando o protocolo POP para que o Agente de Mensagens do Usuário receba as mensagens que estão no

servidor. O passo 1(um) o Agente se identifica colocando as credenciais do usuário, no passo 2(dois) é informado a senha para se autenticar no servidor, no passo 3(três) o Agente solicita através do comando *STAT* o número e o tamanho total das mensagens, no passo 4(quatro) o comando *LIST* solicita o tamanho de uma mensagem específica (se houver), caso contrário o servidor enviará a lista com todas as mensagens, no passo 4(quatro) o servidor retorna com o número da mensagem que foi solicitada no passo anterior, por fim, no passo 5(cinco) o servidor encerra a conexão.

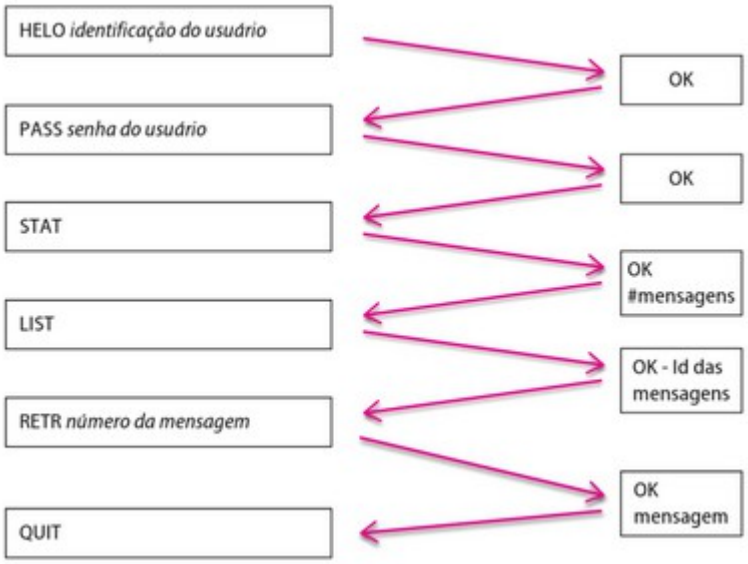

Figura 3: Início da comunicação via POP

Outro protocolo que também pode ser utilizado para este mesmo fim, é o IMAP (Internet Message Access Protocol), Protocolo para Acesso de Mensagens via Internet, preconizado pela RFC 3501, que implementa muitos outros recursos, além das funcionalidades fornecidas pelo POP, destacando-se que as mensagens lidas permanecem no servidor, até que se solicite que sejam excluídas.

O IMAP atua na porta 143 do TCP e na 993 em implementação que utiliza o SSL ou TLS (*Transport Layer Security*), em português significa, Transporte de Canal

Seguro. Vale salientar que o TLS é a evolução do SSL, e que tem por objetivo fornecer segurança nas comunicações via Internet.

A ilustração 4 exemplifica como o Agente de Usuário de Mensagens requisita as mensagens ao Servidor. No passo 1(um) o comando *LOGIN* informa as credenciais do usuário, sendo os parâmetros nome e a senha repassados ao servidor, para que este valide e autorize o acesso, no passo 2(dois) através do comando *LIST* o Agente solicita a Lista de pastas nas quais estão armazenadas as mensagens, no passo 3(três) após o usuário selecionar uma pasta especifica o comando *Examine* é enviado ao servidor no qual este identificará a pasta solicitada e mostrará a(s) mensagem(s) referentes a esta pasta, no passo 4(quatro) o Agente utilizando-se do comando *FETCH* seleciona uma mensagem a ser visualizada, e o servidor responderá apresentando esta mensagem, já no passo 5(cinco) a conexão é encerrada.

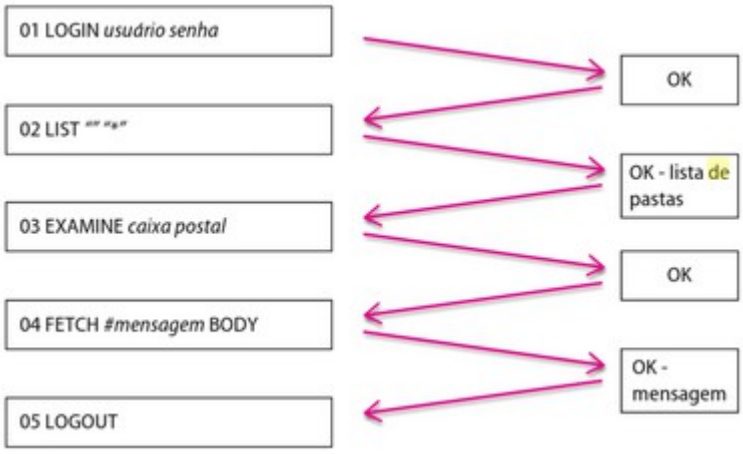

Figura 4: Início da comunicação via IMAP

Os protocolos POP e IMAP são protocolos para recebimento de mensagens, ao contrário do protocolo SMTP, que serve somente para o envio de mensagens.

Para a utilização dos protocolos POP e/ou IMAP, se faz necessária a instalação de um servidor apropriado, que vai ser o responsável por atender as

solicitações do cliente de correio eletrônico. O recebimento de mensagens pelo cliente se dá através da solicitação do Agente de Mensagens do Usuário ao seu servidor de correio eletrônico, que após a autenticação do usuário vai informar se existem mensagens em sua caixa postal e quantas são. A seguir, o MUA solicita a transferência das mensagens para a máquina local, finalizando assim o processo de troca de mensagem entre dois ou mais usuários.

Na figura 5, há dois fluxos nos quais indicam o envio e o recebimento de e-mail. No fluxo 1(um) após ser criado o e-mail o Agente de Mensagens de Usuário (MUA 1) envia ao servidor de correio – Agente Transportador de Mensagem (MTA 1) através do protocolo SMTP o e-mail para que este possa através do destinatário da mensagem localizar o servidor destino (MTA 2) e realizar a entrega da mesma.

Já no fluxo 2(dois), o e-mail ao chegar no servidor destino (MTA 2), este localiza a caixa postal do destinatário (MUA 2), e realiza a entrega da mensagem, utilizando para isso o protocolo POP ou IMAP.

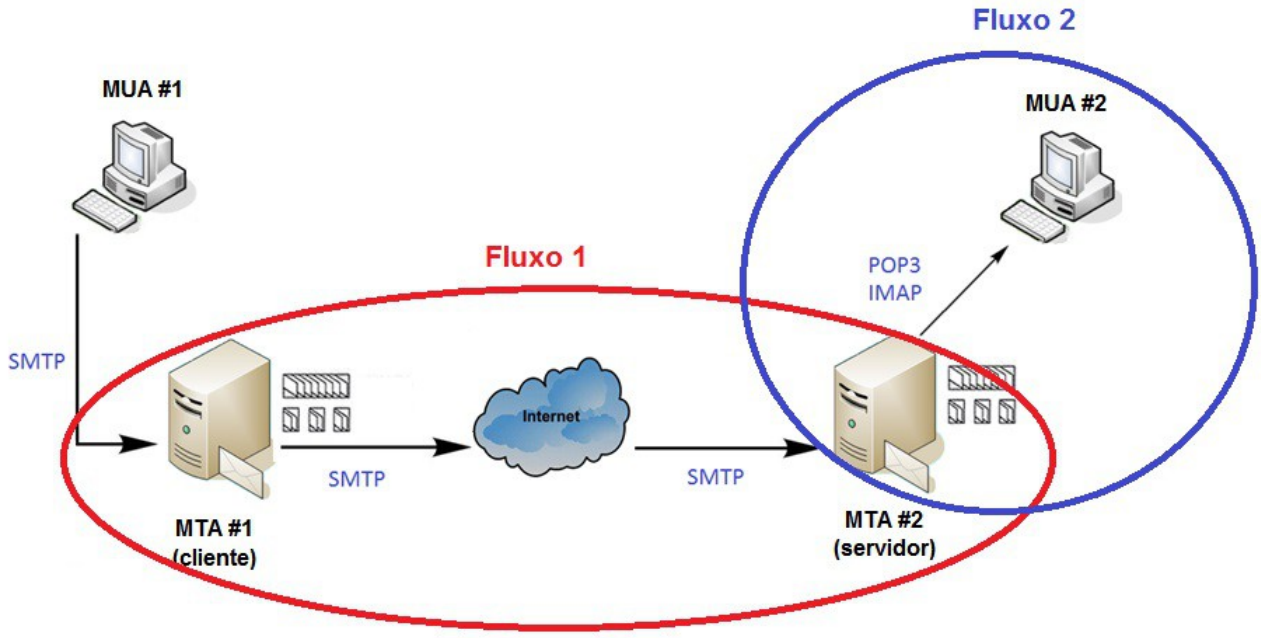

Figura 5: Transmissão de e-mail entre servidores

3.3 CRIPTOGRAFIA

O conceito de criptografia é muito abrangente e bem diversificado, contudo, algumas definições serão mostradas para que se facilite no entendimento acerca do propósito em se criptografar uma mensagem, e como pode ser realizado este processo.

Partindo do ponto de vista terminológico o termo criptografia deriva do latim moderno cryptographia, formado de cript(o), do grego kruptós (“oculto, secreto, obscuro, ininteligível”), mais grafia, do grego -graphía, com o sentido de “escrita”.

No dicionário HOUAISS criptografia significa, “conjunto de princípios e técnicas empregadas para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às convenções combinadas; em operações políticas, diplomáticas, militares, criminais etc., modificação codificada de um texto, de forma a impedir sua compreensão pelos que não conhecem seus caracteres ou convenções”.(HOUAISS, 2009)

De acordo com Steve Burnett e Stephen Paine em seu livro “Criptografia e Segurança – O guia Oficial RSA”, a critptografia é o ato de proteger os dados utilizando métodos e algoritmos que transformam a mensagem legível, em uma mensagem ilegível, fornecendo confidencialidade e autenticidade na comunicação.

Consultando no dicionário da revista especializada, a PC Magazine, esta conceitua criptografia como sendo a técnica de conversão de dados em um código secreto, para transmissão através de rede pública, ou seja, o texto original, ou *plaintext*, é convertido em um equivalente codificado, denominado *ciphertext*, por meio de um algoritmo criptográfico.

Dentro do cenário mundial, a Alliance for Telecommunications Industry

Solutions (ATIS), entende que a criptografia determina os métodos usados para cifração e decifração, no que constitui a:

a) a arte ou ciência que se preocupa com os princípios, meios e métodos de tornar ininteligível a informação, ou de restaurar a informação cifrada, tornando-a inteligível; e

b) a disciplina que incorpora princípios, meios e métodos de transformação de dados, a fim de ocultar o conteúdo da informação, prevenir sua modificação clandestina e/ou prevenir seu uso não-autorizado;

O Institute for Telecommunication Sciences (ITS), ramo de pesquisa e desenvolvimento da National Telecommunications and Information Administration (NTIA), do Departamento de Comércio, já defende que criptografia compreende os princípios, meios e métodos de tornar ininteligível a informação em claro e de restaurar a informação cifrada para uma forma inteligível.

Dos setores especializados brasileiros, a Câmara Brasileira de Comércio Eletrônico, por meio do Grupo de Trabalho de Criptografia Comercial, entende criptografia como a “aplicação de um padrão secreto de substituição dos caracteres, de maneira que a mensagem se torna ininteligível para quem não conhece o padrão criptográfico utilizado”;

Por sua vez, o Instituto Nacional de Tecnologia da Informação (ITI), autarquia federal vinculada a Presidência da República, ensina, didaticamente, que criptografia significa “a arte de escrever em códigos, de forma a esconder a informação na forma de um texto incompreensível”, e que “a informação codificada é chamada de texto cifrado”. Acrescenta, ainda, uma peça fundamental — a chave criptográfica —, por meio da qual são realizadas as operações de cifração e decifração. Aponta que “sem o conhecimento da chave correta não é possível decifrar um dado texto

cifrado.” E finaliza, afirmando que “para manter uma informação secreta, basta cifrar a informação e manter em sigilo a chave”;

Já o Portal ICP Brasil estabelece criptografia como: “Disciplina de criptologia que trata dos princípios, dos meios e dos métodos de transformação de documentos com o objetivo de mascarar seu conteúdo”, afirmando que, é a “ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, através de um processo de cifragem, e para restaurar informações cifradas para sua forma original, inteligível, através do processo de decifragem”.

Além disso, em 2006 o Comitê Gestor da Internet no Brasil (CGIBR), coordenado pelo GSIPR, lançou “Cartilha de Segurança na Internet”, produzida pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), em que define criptografia como: “[...] ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para:

- autenticar a identidade de usuários;
- autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias;
- proteger a integridade de transferências eletrônicas de fundos.”

A cartilha ensina que “Uma mensagem codificada por um método de criptografia deve ser privada, ou seja, somente aquele que enviou e aquele que recebeu devem ter acesso ao conteúdo da mensagem. Além disso, uma mensagem deve poder ser assinada, ou seja, a pessoa que a recebeu deve poder verificar se o remetente é mesmo a pessoa que diz ser, e ter a capacidade de identificar se uma mensagem pode ter sido modificada.” E finaliza sua definição afirmando que “Os métodos de criptografia atuais são seguros e eficientes e baseiam-se no uso de uma

ou mais chaves. A chave é uma sequência de caracteres, que pode conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número, utilizado pelos métodos de criptografia para codificar e decodificar mensagens."

Realizada essas observações, constata-se que a criptografia, seja arte ou ciência, é um processo no qual se executa por meio de duas operações semelhantes e diretamente inversas: cifração e decifração. Estas significam conversão e reversão.

A primeira converte a informação para uma forma ininteligível; a segunda reverte-a para a sua forma original. Isso é possível com a aplicação de uma chave criptográfica ao texto.

Pode-se esquematizar de maneira bem sucinta, criptografia da seguinte forma:

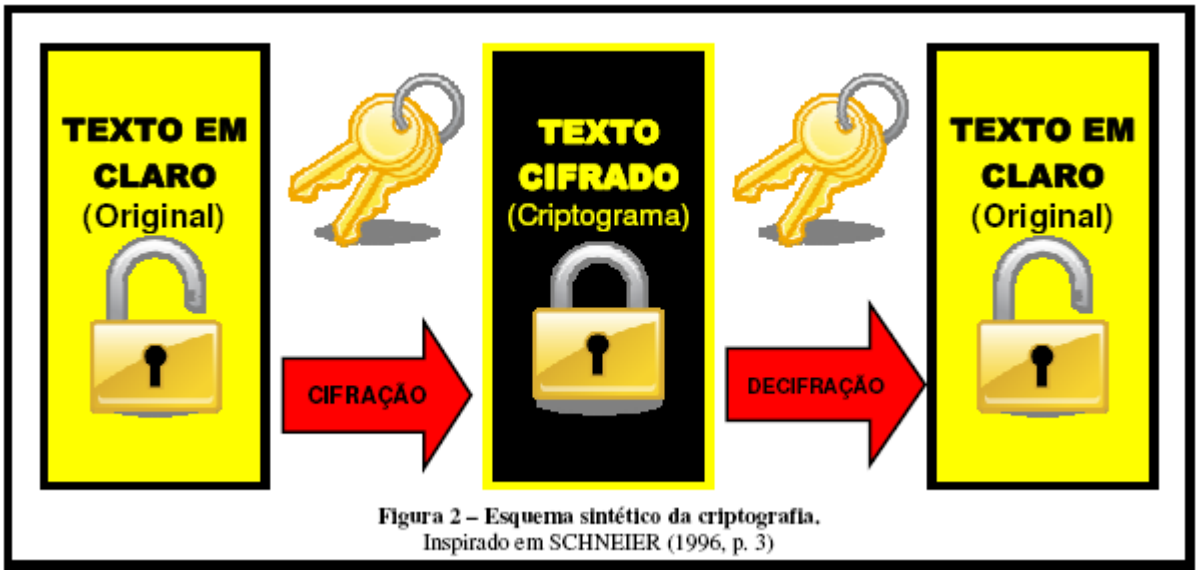

Figura 6: Processo simplificado de cifração e decifração de texto

Logo, para os efeitos deste trabalho, considera-se criptografia, ou cifração, como técnica ou conjunto de técnicas que possibilita, com o emprego de chave cifradora/decifradora, tornar ininteligíveis textos em claro e, inversamente, tornar

inteligíveis textos cifrados, de forma a proteger a informação contra acesso não autorizado ao seu conteúdo, provendo a confidencialidade e integridade das informações.

Existem duas classes de algoritmos criptográficos: ***simétricos*** (ou de ***chave-secreta***) e ***assimétricos*** (ou de ***chave-pública***).

Os algoritmos simétricos utilizam uma mesma chave tanto para criptografar como para descriptografar, ou seja, fazendo uma analogia, a mesma chave utilizada para “fechar o cadeado” é utilizada para “abrir o cadeado”.

Nos algoritmos assimétricos obtêm-se chaves distintas, uma para criptografar e outra para descriptografar e, além disso, a chave de descriptografia não pode ser obtida a partir do conhecimento da chave de criptografia apenas. Aqui, uma chave é utilizada para “fechar” e outra chave, diferente, mas relacionada à primeira, tem que ser utilizada para “abrir”. Por isso, nos algoritmos assimétricos, as chaves são sempre geradas aos pares.

Os algoritmos simétricos exigem que a chave seja mantida secreta, do conhecimento exclusivo dos dois interlocutores. Este fato traz complexidade ao manuseio destas chaves, o que dificulta um pouco a utilização destes algoritmos isoladamente.

É requerido antes de iniciar a troca de chave, o estabelecimento de um canal seguro no qual permita a um usuário transmitir a chave ao seu interlocutor. A figura 7 demonstra a forma de operação do algoritmo criptográfico simétrico, onde o interlocutor Bob envia uma mensagem cifrada para Alice, tendo antes que enviar a chave que vai utilizar, secretamente, para Alice.

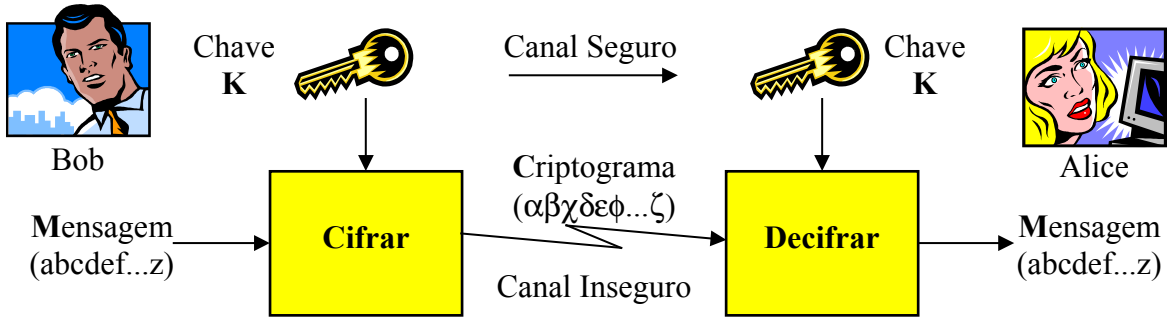

Figura 7: Uso de algoritmo criptográfico simétrico (chave secreta).

Já nos algoritmos assimétricos a chave de cifração e/ou decifração pode se tornar pública, por exemplo, disponibilizando-a em um repositório de acesso público, o que é conhecida como chave-pública, retirando aquele problema existente nos algoritmos simétricos. Qualquer um pode cifrar mensagens com uma dada chave-pública, contudo somente o destinatário, detentor da correspondente chave de decifração (denominada chave-privada, ou secreta), poderá decifrá-la.

A chave-privada não pode ser dada e nem conhecida por ninguém, devendo ser guardada em segredo pelo seu detentor apenas, no qual deve também ter sido o responsável pela geração do seu par de chaves, enquanto a chave-pública pode ser publicada livremente.

Explicando melhor a forma de operação do algoritmo assimétrico, a figura 8 mostra que Alice gera seu par de chaves, e envia (publica) sua chave-pública para Bob, este por sua vez, cifra a mensagem com a chave-pública de Alice ($K_{Pública}$), a qual, e somente ela, será capaz de decifrá-la, utilizando sua chave-privada ($K_{Secreta}$).

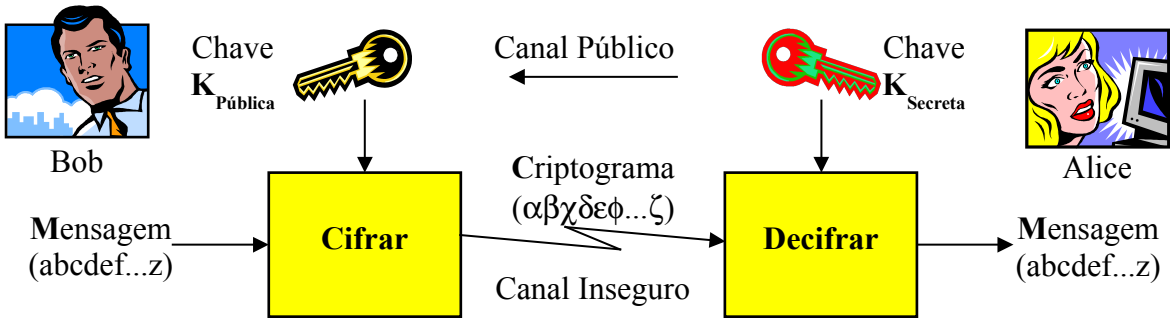

Figura 8: Uso de algoritmo criptográfico assimétrico (chave pública).

Geralmente os algoritmos simétricos são mais eficientes computacionalmente que os assimétricos, podendo ser bastante rápidos em sua execução, permitindo altas taxas de cifração (até da ordem de gigabits/s – 10^9 bits/s).

Os algoritmos assimétricos são geralmente menos eficientes, porém mais seguros no que diz respeito a troca e armazenamento de chaves, e normalmente a tendência é a utilização dos dois tipos de algoritmos em conjunto, tal que o algoritmo de chave-pública é utilizado para cifrar a chave criptográfica simétrica gerada aleatoriamente, e esta é utilizada para cifrar a mensagem.

O destinatário então primeiro decifra a chave simétrica utilizando sua chave-privada no sistema de chave-pública, e após isto, decifra a mensagem utilizando a chave recuperada no sistema simétrico. Desta forma não há problema em "compartilhar o segredo da chave" com ninguém.

A cada nova mensagem pode-se sempre repetir todo o processo.

A figura 9, ilustra esta situação, mostrando o processo de transmissão utilizando estes dois métodos criptográficos. Então, se Bob deseja enviar uma mensagem para Alice, ele primeiro escolhe uma chave K, e a envia através do algoritmo de chave-pública cifrada com a $K_{Pública}$ de Alice. Esta recupera K decifrando o criptograma recebido com sua chave privada $K_{Secreta}$. Agora Bob pode enviar a mensagem real através do algoritmo simétrico, mais eficiente para isto, cifrando-a com a chave K, que Alice já dispõe, e enviada a ela de forma segura.

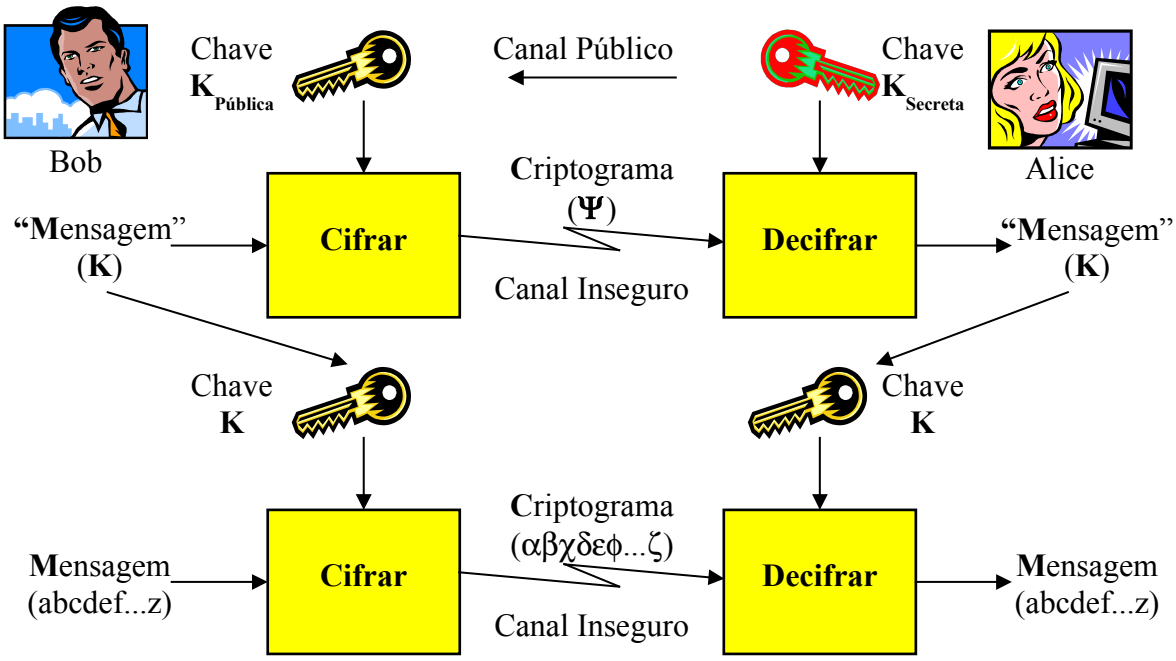

Figura 9: Uso de misto de algoritmo criptográfico assimétrico e simétrico.

3.4 ICP BRASIL

A ICP Brasil (Infraestrutura de Chaves Pública Brasileira) é uma cadeia hierárquica e de confiança, em que viabiliza a emissão de certificados digitais através de um conjunto de entidades, padrões técnicos e regulamentos.

Foi instituída através da medida provisória 2.200-2 de 24 de agosto de 2001, com o objetivo de garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais.

Para gerir a ICP, foi criado o Comitê Gestor, que se vincula à Casa Civil da Presidência da República, composto por 5 representantes civis e um membro de cada órgão: Ministério da Justiça, Ministério da Fazenda, Ministério do Desenvolvimento, Indústria e Comércio Exterior, Ministério do Planejamento, Ministério da Ciência e Tecnologia, Casa Civil e Gabinete de Segurança da Presidência da República.

Na estrutura estabelecida pelo ITI (Instituto Nacional de Tecnologia da Informação) órgão responsável pela coordenação da ICP Brasil, determina que a AC Raiz (Autoridade Certificadora Raiz) é a primeira autoridade da cadeia de certificação, e que possui as seguintes atribuições: de emitir, distribuir, revogar, gerenciar os certificados das autoridades certificadoras de nível abaixo e executar as políticas de certificação, bem como definir normas técnicas e operacionais para com essas AC's.

É atribuição da AC Raiz também emitir a lista de certificados revogados (LCR) e de fiscalizar e auditar as Autoridades Certificadoras, Autoridades de Registros e demais prestadores de serviço habilitados na ICP-Brasil.

A Autoridade Certificadora (AC) é uma entidade pública ou privada, na qual se subordina à hierarquia da ICP Brasil, ou seja, está abaixo da AC Raiz.

Tem como responsabilidades a de emitir, distribuir, renovar, revogar e gerenciar certificados digitais, bem como verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado.

Cabe também a AC, emitir listas de certificados revogados (LCR) e manter os registros de suas operações, além de estabelecer e fazer cumprir regras para as Autoridades de Registros subordinadas a ela.

As Autoridades de Registros (AR) tem por objetivo identificar, cadastrar usuários, e encaminhar as solicitações de certificados para as AC's.

Há também uma Autoridade na qual atesta o tempo em que o certificado foi utilizado e/ou emitido, esta é denominada de Autoridade Certificadora de Tempo, tem por finalidade fornecer carimbo de tempo, que é um conjunto de atributos fornecidos pela parte confiável do tempo (ano, mês, dia, hora, minuto e segundo) que, associado a uma assinatura digital, confere provar a sua existência em determinado período.

Toda esta estrutura se deu, devido a expansão no uso de certificados digitais que cresceu de maneira exponencial no início do século XXI.

A Certificação Digital permite que informações trafeguem pela Internet com maior segurança, evitando por exemplo que hackers interceptem ou adulterem as comunicações.

Também é possível identificar quem foi o autor de uma transação ou de uma mensagem, ou, ainda, manter dados confidenciais protegidos contra a leitura por pessoas não autorizadas.

As principais vantagens de se utilizar o certificado digital são:

- Garantia de sigilo e privacidade – Quando acessa um site "seguro" da web, o computador recebe um certificado contendo a chave pública deste site, o que é suficiente para criar um túnel criptográfico, tornando os dados incompreensíveis durante o tráfego, sendo possível apenas ao servidor web recuperar a informação original.
- Controle de acesso a aplicativos – O servidor web pode solicitar ao usuário que apresente um certificado digital, em vez de digitar usuário e senha. Os usuários não poderão colocar em perigo a aplicação pela falta de cuidado no uso e armazenamento da senha.
- Assinatura de formulários e impossibilidade de repúdio – Os usuários podem assinar os formulários que submetem preenchidos pela web da mesma maneira que fariam pessoalmente em um balcão de atendimento. Além disso, qualquer documento digital passa a valer como documento assinado, com validade jurídica, dispensando-se o uso de papel.
- Garantia de integridade e confidencialidade – O sistema de correio eletrônico utilizado para troca de mensagens através da Internet não possui recursos nativos para impedir a violação da correspondência eletrônica. Com a utilização de certificados digitais, a mensagem criada é envelopada em meio digital criptográfico e com isso, certifica-se de que apenas o destinatário será capaz de compreender seu conteúdo.
- Identificação do remetente – O autor não poderá se eximir da culpa, alegando que não foi ele em que executou tal atividade dentro de um sistema, no qual utilize o certificado digital, uma vez que a utilização do certificado é realizada de maneira pessoal e intransferível.

3.5 HSM

De acordo com a FIPS, nomenclatura para *Federal Information Procesing Standard,* ou seja, Padrão de Processamento de Informação Federais, publicado pelo Instituto Nacional de Padrões e Tecnologia, tem por objetivo definir e especificar os requisitos de segurança que o módulo criptográfico precisa atender, apontando também sua composição na qual dá em Hardware, Software e Firmware, e os processos e funções criptográficas que podem ser implementadas, sendo este padrão mundialmente reconhecido.

Estes requisitos são divididos em 4 níveis de segurança:

Nível 1: este é o menor nível de segurança,

Nível 2: aperfeiçoa os mecanismos de segurança do nível 1 e acrescenta recursos que mostram evidência de adulteração do dispositivo, incluindo sensores que detectam a violação física ao módulo;

Nível 3: acrescenta aos mecanismos de nível 1 e 2 funções relativas a detecção e resposta às tentativas de acesso físico ao módulo criptográfico, estas funções incluem uso de caixa-forte e adulteração de detecção de circuitos

Nível 4: este é o mais alto nível de segurança, agregando mecanismos que além de detectarem invasão, eliminam as tentativas, proporcionando até mesmo uma proteção ao comprometimento da segurança devido às condições ambientais ou flutuações fora de intervalos normais de funcionamento do módulo de tensão e temperatura.

Os Módulos de Segurança Criptográficos (Hardware Security Module ou HSM da sigla em inglês) podem prover um grande número de funcionalidades, tais como: geração e armazenamento seguro de chaves criptográficas, verificação de assinaturas digitais, aceleração de conexões utilizando o protocolo SSL, criptografia

de dados, verificação de integridade de dados e registros de auditoria.

O HSM possui controles que fornecem evidências de adulteração, como registros de logs e mecanismos avançados de detecção e de violação do hardware.

Pode ser classificado de três maneiras distintas, de acordo com suas características, são elas:

- HSM Embarcado

É um modelo do tipo FIPS 140-2 – (*Multiple-chip embedded cryptographic module)*, ou seja, Módulo Criptográfico Embarcado de Múltiplas Conexões, no qual o módulo executa as funções de segurança, porém não funciona separado, é necessário ser acoplado em uma máquina, utilizando para isso, interface PCI ou PCI-Express, contudo, em alguns casos pode ser utilizada também USB.

Sua proteção se dá através de software, como por exemplo, a análise de tempo das operações criptográficas[1]

Figura 10: Exemplo de HSM Embarcado

- HSM Standalone

Neste modelo, os dispositivos têm autonomia sobre suas responsabilidades e executa suas funções à parte de outras máquinas.

A proteção física é realizada em todo o módulo, e isso é feito de

1 Segundo a FIPS 140-2 – Análise de tempo baseia-se em medir o tempo que o módulo leva para executar as operações matemáticas de cada algoritmo criptográfico, essa informação pode ser utilizada para encontrar uma relação entre as chaves e as entradas usadas, podendo ser explorada para revelar as chaves criptográficas

diversas formas, podendo ter blindagens de aço ou material semelhante contra perfurações e abertura do módulo, podendo inclusive ter proteções de blindagem elétrica, através de sensores que servem para mitigar ataques de indução à falha, conhecido como TEMPEST[2]

Figura 11: Exemplo de HSM Standalone

- HSM em rede

Modelo de HSM Standalone que fornece serviços a uma rede de computadores, fazendo com que as máquinas da rede possam utilizar os recursos dos HSM de modo compartilhado, para tanto, faz-se necessário a utilização de balanceadores de carga para poder de maneira igualitária distribuir as solicitações de recursos de segurança entre os HSMs.

Figura 12: Exemplo de HSM em rede

2 Segundo a noma FIPS 140-2: Ataques Tempest envolvem a detecção externa de sinais eletromagnéticos emitidos pelo módulo durante o processamento. Isto é qualquer processamento de informações dentro do módulo, geram ondas eletromagnéticas que eventualmente saem do módulo e podem ser capturadas por um agente externo, estas ondas podem ser transformadas em informações ou dar indícios que levem a descoberta da chave, por exemplo.

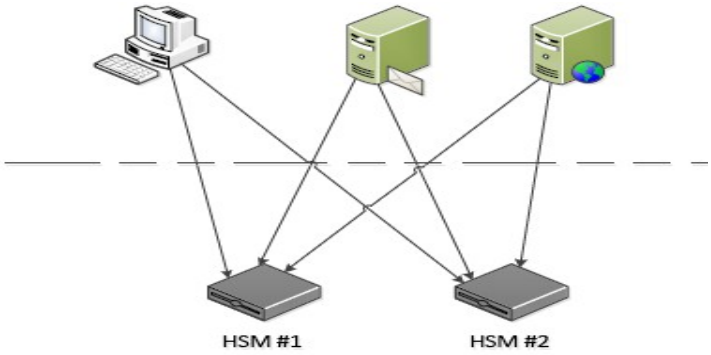

Figura 13: Cenário de utilização do HSM em rede

Para a execução das funções dentro do HSM, são criados diferentes tipos de grupos, que realizam determinadas funções:

Grupo de Administração: Se limita a apenas 1 (um) dentro do HSM, pois este é o perfil responsável por criar todos os outros grupos do HSM, porém existe a possibilidade de se alterar o grupo existente, criando um grupo novo e excluindo o existente.

O tamanho deste grupo é definido no momento da sua criação, logo, o grupo deve ter um valor M, que é o número máximo de participantes, e um N, que é o número de participantes necessários para a autenticação, tal que $1 \leq N \leq M$.

Suas principais funções são:

- Apagar configurações;
- Atualizar firmware;
- Desligar o módulo HSM;
- Alterar data/hora;
- Gerar/Recuperar backup;
- Gerar par de chaves assimétricas.

Grupo de Auditoria: este grupo tem a responsabilidade de verificar o bom andamento das operações do módulo, não é limitado a apenas um grupo de auditoria, porém é necessário que se tenha ao menos um dentro do módulo.

Suas atribuições são:

- Exportar logs;
- Bloquear o equipamento;
- Recuperar backup.

Grupo de operação: este é o grupo responsável por gerenciar o uso das chaves criptográficas, isso significa determinar quando e quantas vezes as chaves que estão a cargo de cada grupo de operação poderá ser utilizada.

Suas funções são:

- Carregar chave para uso;
- Definir políticas de utilização da chave
    - Tempo de uso
    - Quantidade de utilização

Vale salientar que existem algumas operações dentro do módulo HSM, que não necessitam de autenticação por se tratarem de operações onde não existem o tráfego de informações sigilosas, tais como: verificar versão do software, mostrar seu estado atual, realizar auto-teste, listar grupos.

3.5.1 BACKUP

A função de Backup garante a continuidade das chaves privadas

armazenadas, mesmo na eventual falha do equipamento e/ou a destruição das mesmas.

O procedimento se dá através da obtenção de um pacote de arquivos que é cifrado com a chave pública do outro HSM, isso é necessário para garantir que o pacote de backup gerado só possa ser restaurado no HSM que mantém a chave privada desse par.

Dentro deste pacote de arquivos, estão contidas informações referentes às configurações do HSM, grupos de gerência, chaves gerenciadas, entre outros dados.

Para ser realizado a restauração do pacote de backup é necessário a autenticação do grupo de administradores e de um grupo de auditores.

3.5.2 BIBLIOTECA OPENSSL

Para realizar as funções providas pelo HSM, se faz uso da biblioteca OpenSSL, no qual ela pode ser carregada por um programa, ou pode ser carregada em linha de comando.

No momento que se inicia a função, o protocolo SSL se comunica com o HSM, executando a função criptográfica requisitada.

As principais funções OpenSSL providas pelo HSM são:

openhsmd_load_private_key: utilizada para carregar uma chave privada

openhsmd_load_public_key: utilizada para carregar uma chave pública

openhsmd_engine_private_decrypt – utilizada para decifrar dados

openhsmd_engine_private_encrypt: utilizada para cifrar dados

4. SOLUÇÃO DE AUDITORIA PROPOSTA

4.1 A SOLUÇÃO

Com a problemática trazida pelo trabalho, foi elaborada uma solução que contempla uma tecnologia moderna, processos bem definidos, procedimentos estabelecidos entre todos os envolvidos e sobretudo que esteja respaldado por legislação e normas internas da empresa, com isso o sistema proposto, foi a implementação do módulo criptográfico (HSM) integrado ao correio eletrônico para propiciar assim uma auditoria de quebra de sigilo segura e confiável.

O trabalho foi árduo e cheio de entraves, pois, por ser esta uma empresa governamental, os meios legais têm que estarem de acordo com as determinações e resoluções jurídicas que permitam e assegurem a instituição realizar procedimento de auditoria.

Para isso, foi necessário o envolvimento de várias áreas da organização para que pudesse ser desenvolvido um sistema que se adequasse tanto ao meio tecnológico, quanto aos meios jurídicos legais, no que diz respeito a violação da mensagem criptografada, por parte de pessoas que teoricamente não tiveram participação nesta troca de mensagem.

Contou-se também com a colaboração de especialistas na parte do módulo criptográfico de uma Universidade Federal, e aqui ressalto a grande importância que eles tiveram, pois as bibliotecas OpenSSL utilizadas para a criptografia e descriptografia foram providas e desenvolvidas por eles.

Já no âmbito interno da organização, pessoas do departamento de segurança da informação, de desenvolvimento do correio eletrônico, de operação da sala-cofre, da gestão de pessoas e gestão jurídica reuniram-se ao longo de 1 (um) ano para

elaborarem normativos e procedimentos técnicos, com o objetivo de fornecerem insumos ao processo de auditoria de quebra de sigilo, para que este fosse efetivado e tivesse todo o respaldo jurídico necessário. Os seguintes objetivos foram traçados e estabelecidos:

- Razões pautadas em leis e normas internas para que pudesse ser auditado e-mail criptografado;
- Número necessário de pessoas para fazerem parte do processo de auditoria de quebra de sigilo, conhecido como custodiantes;
- Áreas envolvidas neste processo;
- Local de armazenamento dos módulos de HSM;
- Elaboração de processo para criação e utilização das chaves privadas/públicas;
- Integração do certificado de sigilo junto ao correio eletrônico;
- Cerimônia de descriptografia e quebra de sigilo de mensagens.

Após o estabelecimento destes objetivos, deparamos com um ponto crítico e que vale a pena ser ressaltado, a questão da classificação de mensagens.

Esta classificação é estabelecida através da Lei de Acesso a Informação de 18 de novembro de 2011, mais conhecida como LAI, em que separa as informações em 3 tipos: ultrassecretas, secretas e reservadas em que cada uma possui seu grau de sigilo.

São consideradas informações:

Ultrassecretas: às referentes à soberania e à integridade territorial nacional, a planos e operações militares, às relações internacionais do país, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não-autorizado possa acarretar

dano excepcionalmente grave à segurança da sociedade e do Estado.

Secretas: às referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não-autorizado possa acarretar **dano grave** à segurança da sociedade e do Estado.

Reservadas: cuja revelação não-autorizada possa **comprometer** planos, operações ou objetivos neles previstos ou referidos.

Através dessa classificação poderão ser utilizados dois tipos de algoritmos para a criptografia:

- Algoritmo de Estado: função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades do Poder Executivo federal;
- Algoritmo Registrado: função matemática utilizada na cifração e na decifração de informações não classificadas, para uso exclusivo em interesse do serviço de órgãos ou entidades da Administração Pública Federal, direta e indireta, cujo código fonte e método de processo sejam passíveis de controle e auditoria.

Logo, este trabalho foi baseado somente na utilização de Algoritmo Registrado, uma vez que o objetivo desta solução é prover auditoria para mensagens que foram concebidas por empregados da instituição das quais estas não são classificadas como ultrassecreto ou secreto, pois para estas terão que utilizar criptografia de Estado, além do mais, a própria LAI determina que para a utilização destas classificações acima só são permitidas para pessoas que sejam:

- Grau ultrassecreto

a) Presidente da República;

b) Vice-presidente da República;

c) Ministros de Estado e autoridades com a mesma prerrogativa;

d) Comandantes da Marinha, Exército e Aeronáutica;

e) Chefes de Missões Diplomáticas e Consulares permanentes no exterior.

- Grau Secreto

  Das autoridades que podem classificar informações em grau ultrassecreto, além dos titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista.

Estas definições foram importantes e norteadoras para a perfeita compreensão dos objetivos desta solução, e que com isso finalizar todos os requisitos para o desenvolvimento do sistema, fazendo com que este utilize o algoritmo registrado para a criptografia das mensagens.

Este sistema conta com a utilização de 3 (três) HSMs que ficam isolados da rede da organização, atuando de forma *Offline*, sendo que 2 (dois) são para o ambiente de produção no qual um deles servirá de backup, e o outro como desenvolvimento e homologação desta solução.

Esta forma de atuação é justamente para que eles possam apenas criar chave privada e pública e o certificado de sigilo, não tendo a necessidade de atuação fora desse escopo.

Os HSMs por serem considerados equipamentos que provêm mecanismos de segurança, foram instalados dentro de sala cofre, como bem preconiza o normativo DOC-ICP-10 terceira versão de 27 de setembro de 2012 da ICP Brasil, na qual determina as condições necessárias para instalação física.

A sala-cofre provê várias formas de proteção física, necessárias a guarda e utilização da chave privada que fica dentro do HSM.

Possui capacidade de fornecer um ambiente físico seguro, por constituir-se de um aparato tecnológico e eletrônico moderno, formado por vários subsistemas, tais como: fornecimento de energia elétrica redundante e ininterrupta, detecção e combate a incêndio, monitoração do ambiente e climatização apropriada, que juntos fornecem proteção contra: umidade, poeira, fogo, desmagnetização, vandalismos e gases corrosivos provenientes do ambiente externo

Este ambiente é projetado e construído em conformidade com as normas da Associação Brasileira de Normas Técnicas – ABNT em conjunto com as do INMETRO, ABNT NBR 11515 de 2007 e ABNT NBR 15247 de 2004.

Também, foi necessária a criação de um normativo para pontuar em quais situações o processo de quebra de sigilo da mensagem criptografada se faz presente, e de outro lado, respaldar a organização para tal procedimento.

Nesta norma preconizou os possíveis casos dos quais se submeterão ao processo de auditoria, são eles:

- Ordem judicial, fundamentado aqui através do art. 10º §2 da lei 12.965 de 23 de abril de 2014, conhecida como Marco Civil da Internet;
- Investigação interna sobre Processo Administrativo – PAD;
- Perda das chaves privadas;
- Falecimento das partes;
- Afastamento do trabalho por motivo de doença ou viagem que demore muito o regresso;
- Férias;
- Auditoria interna.

Por outro lado, também tiveram os fatores que contribuíram para que a organização se respaldasse em caso de utilizar-se do processo de auditoria, são eles:

- Decreto presidencial nº 8.135 de 04 de novembro de 2013;
- Portaria nº 54 da Secretaria de Logística e Tecnologia da Informação – Ministério do Planejamento;
- Instrução Normativa nº3 do Gabinete de Segurança Institucional da Presidência da República.

O custo desta solução se dá primordialmente na aquisição dos HSM's, caso em que a organização já possua uma sala-cofre para guarda destes equipamentos.

4.2 INTEGRAÇÃO DO HSM COM O CORREIO ELETRÔNICO

Após ter o entendimento acerca de como é o funcionamento do HSM, bem como os conceitos de chaves criptográficas, certificados digitais e correio eletrônico, será apresentada então a forma de integração entre o módulo HSM com o correio eletrônico.

Inicialmente se faz necessária a criação do chamado Grupo de Custódia – nome este utilizado, devido a resolução 39 (trinta e nove) de 18 de abril de 2006 da ICP Brasil -, no qual tem por objetivo fornecer maior confiabilidade ao processo de auditoria de quebra de sigilo, fazendo com que haja um compartilhamento de responsabilidades, no sentindo de que as pessoas envolvidas neste grupo devem validar e certificar que a cerimônia de descriptografia ocorreu de maneira segura e confiável, ou seja, a mensagem foi submetida ao procedimento de descriptografia de forma legal.

Para isso, foram envolvidos empregados de várias áreas da organização, podendo até mesmo ser de fora dela.

Estes geralmente possuem funções gerenciais e/ou cargo de confiança, pois como as mensagens que se submeterão a este processo, são na maioria das vezes decorrentes de processos administrativos e/ou judiciais, nos quais requerem um alto grau de sigilo, e seu teor é por muitas vezes de caráter confidencial, é muito importante então que sejam elencadas pessoas, nas quais têm a responsabilidade e o dever de manter este sigilo da informação.

Foram então selecionados gerentes das áreas: jurídica, segurança da informação, administração do correio eletrônico, gestão de pessoas e operação do hardware criptográfico para que compusessem o grupo de custódia. Estes

empregados foram selecionados através das características que foram citadas acima, e também pela determinação da diretoria da empresa, na qual, acha essencial que estas áreas estejam totalmente integradas e envolvidas neste processo.

O processo de criação se inicia com a convocação destes empregados, que são chamadas aqui de custodiantes, e podem ser representados pelo valor “M” no qual corresponde a quantidade de membros que fazem parte deste grupo, isto é estabelecido a critério de cada organização.

Com base neste grupo, é determinado o valor “N” no qual corresponde ao número mínimo de custodiantes que devem fazer parte do processo para criar as chaves públicas/privadas, bem como a geração do certificado de sigilo e acionar a chave privada no processo de auditoria da mensagem.

Logo, esta relação fica categorizada como M > N, por exemplo, em uma corporação podem ser escolhidos para serem custodiantes 15 (quinze) empregados, que são oriundos de várias áreas da empresa, inclusive de fora dela. E para ativar as funções descritas acima serão necessárias ao menos 3 (três) custodiantes, pois, a relação 15 > 3 faz com que este quorum mínimo de 3 (três) possam executar as funções com a chave privada.

A segurança ao acesso no HSM por parte dos custodiantes se dá através de Smartcards em que cada um terá o seu, possuindo sua senha pessoal e intransferível, sendo que estes também são armazenados dentro da sala-cofre.

No primeiro momento, ou seja, o de criação do grupo de custodiantes, todos estes devem estar presentes e de posse de seus respectivos Smartcards, após este momento, as outras operações poderão ser realizadas com o número “N” de custodiantes.

O processo de convocação dos custodiantes para as atividades descritas acima é conhecido como cerimônia. Nesta cerimônia, o operador do módulo HSM segue um rito criterioso, que vai deste a identificação de cada custodiante até a emissão do certificado ou utilização da chave privada.

Após a etapa de habilitação de custodiantes dentro do módulo do HSM, a próxima fase é a geração das chaves públicas e privadas dentro deste.

Aqui vale um adento no que diz respeito à proteção da chave privada, para isto, utiliza-se mecanismos de segurança física com o objetivo de impedir o acesso ao seu interior, e assim garantir a integridade evitando uso, modificação ou substituição não autorizada de componentes do HSM, para que se evidencie, resista, detecte e responda a violação.

Para cumprir com este objetivo, o módulo HSM dispõe de circuito “supervisor” que registra e responde à violações, porém a resposta vai depender do modo de operação que estiver configurado no equipamento, mas de forma geral, se este estiver ligado, será procedida a destruição da Chave Mestra na memória volátil e iniciar o imediato desligamento do equipamento.

Já no caso do equipamento se encontrar no estado desligado, o circuito supervisor irá somente registrar a violação. Este circuito dispõe de bateria interna, para manter a memória volátil que armazena parâmetros críticos de segurança, um sub-circuito de gerenciamento de energia faz com que a carga da bateria só precise ser utilizada quando o equipamento estiver desligado da fonte de energia AC e no caso de violação a bateria é desconectada.

Para realizar a ativação do HSM seguinte à violação, são analisados dois modos de operação: FIPS e non-FIPS. No modo FIPS, o equipamento não poderá ser mais utilizado, já no caso de estar como non-FIPS o operador será avisado

sobre a violação e terá a opção de continuar operando, mas o HSM não poderá ser colocado em nenhum momento posterior em modo FIPS.

O único meio de acesso físico autorizado ao interior do HSM é através da remoção da tampa de manutenção superior, onde esta tampa é protegida por sensores que detectam tentativas de remoção. A ativação destes sensores inicia imediatamente o processo de destruição de informações não cifradas da memória e o desligamento do HSM.

Voltando então a fase de geração de chaves pública/privada, esta acontece no momento em que o número “N” de custodiantes se habilita no módulo do HSM, utilizando seus Smartcards (cartões eletrônicos utilizados para autenticação) para a validação, e inicia o procedimento para a geração das chaves, esta fase é realizada em conjunto com o operador do módulo HSM que através da console do equipamento executa as funções presentes para geração das chaves.

Após este momento, passa-se para a criação do certificado de sigilo, que será utilizado no correio eletrônico no momento da criptografia da mensagem. Este certificado é criado também através dos custodiantes nos quais fazem uso da chave privada que fora gerada, nota-se que como o universo “M” de custodiante é maior do que o valor “N” necessário para executar algumas funções já mencionadas acima, não necessariamente precisa ser os mesmos que participaram da cerimônia de geração da chave privada, que participem do processo de criação do certificado de sigilo e até mesmo da utilização da assinatura com a chave privada.

Todos estes processos podem ser realizados em momentos distintos e com diferentes custodiantes, desde que tenha o quórum mínimo necessário para executar as funções.

Vale lembrar que o certificado de sigilo é utilizado para proporcionar o sigilo

ou criptografia de dados, e sua aplicabilidade se dá na codificação de documentos, de base de dados, de mensagens e de outras informações sigilosas.

A ICP-Brasil classifica os certificados em 8 tipos dentro de 2 séries em que contém 4 tipos em cada série.

Na série “A” (A1, A2, A3 e A4) são certificados de assinatura digital, utilizados para a confirmação de identidade de um sítio na web, redes virtuais privadas (VPN) e em documentos eletrônicos que necessitam de verificação da integridade de suas informações.

Já na série “S” (S1, S2, S3 e S4) são certificados de sigilo, que tem como objetivo serem utilizados na codificação de documentos, de bases de dados, de mensagens e de outras informações eletrônicas sigilosas.

A figura 14 mostra os tipos de certificados, com suas respectivas características.

Tipo de certificado	Chave Criptográfica			Validade Máxima (anos)
	Tamanho (bits)	Processo de geração	Mídia armazenadora	
A1 e S1	2048	Software	Arquivo	1
A2 e S2	2048	Software	Smartcard ou Token, sem capacidade de geração de chave	2
A3 e S3	2048	Hardware	Smartcard ou Token, com capacidade de geração de chave	5
A4 e S4	4096	Hardware	Smartcard ou Token, com capacidade de geração de chave	6

Figura 14: Tipos de certificados – Tabela retirada da ICP Brasil

A partir da criação do certificado de sigilo, dar-se-á o processo de colocá-lo junto ao ambiente do correio eletrônico, para que no momento que for realizado a criptografia entre as partes (usuário A e B por exemplo), vá também o certificado gerado pelo HSM.

A partir deste momento, sempre que o usuário for enviar um e-mail criptografado, o sistema de correio eletrônico acoplará junto o certificado de sigilo gerado pelo HSM, ou seja, no S/MIME que é entendido como protocolo para envio de mensagens assinadas e criptografadas digitalmente, a mensagem enviada, terá tanto a chave pública do destinatário, quanto a do HSM.

A figura 15 ilustra a forma de composição de e-mail criptografado.

O passo 1(um) o usuário redige o e-mail, colocando o conteúdo e os destinatários. Como o e-mail será criptografado, ao inserir os destinatários e requisitado ao servidor (passo 2) que este encaminhe os certificados públicos dos destinatários.

No passo 3(três) o servidor busca os certificados no banco de dados, valida a data de expiração, as cadeias de certificação e a lista de revogação, após isto, entrega ao cliente, incluindo o certificado S3 gerado pelo HSM que é do grupo de custódia.

No passo 4(quatro) o cliente (remetente da mensagem) recebe os certificados dos destinatários e envia o seu próprio certificado público ao servidor, para que nos passos 5 e 6 (cinco e seis) possam realizar a mesma validação que fez no passo 3(três).

No passo 7(sete) a mensagem é criptografada e enviada (passo 8).

O servidor (passo 9) recebe a mensagem e encaminha aos destinatários (passo 10).

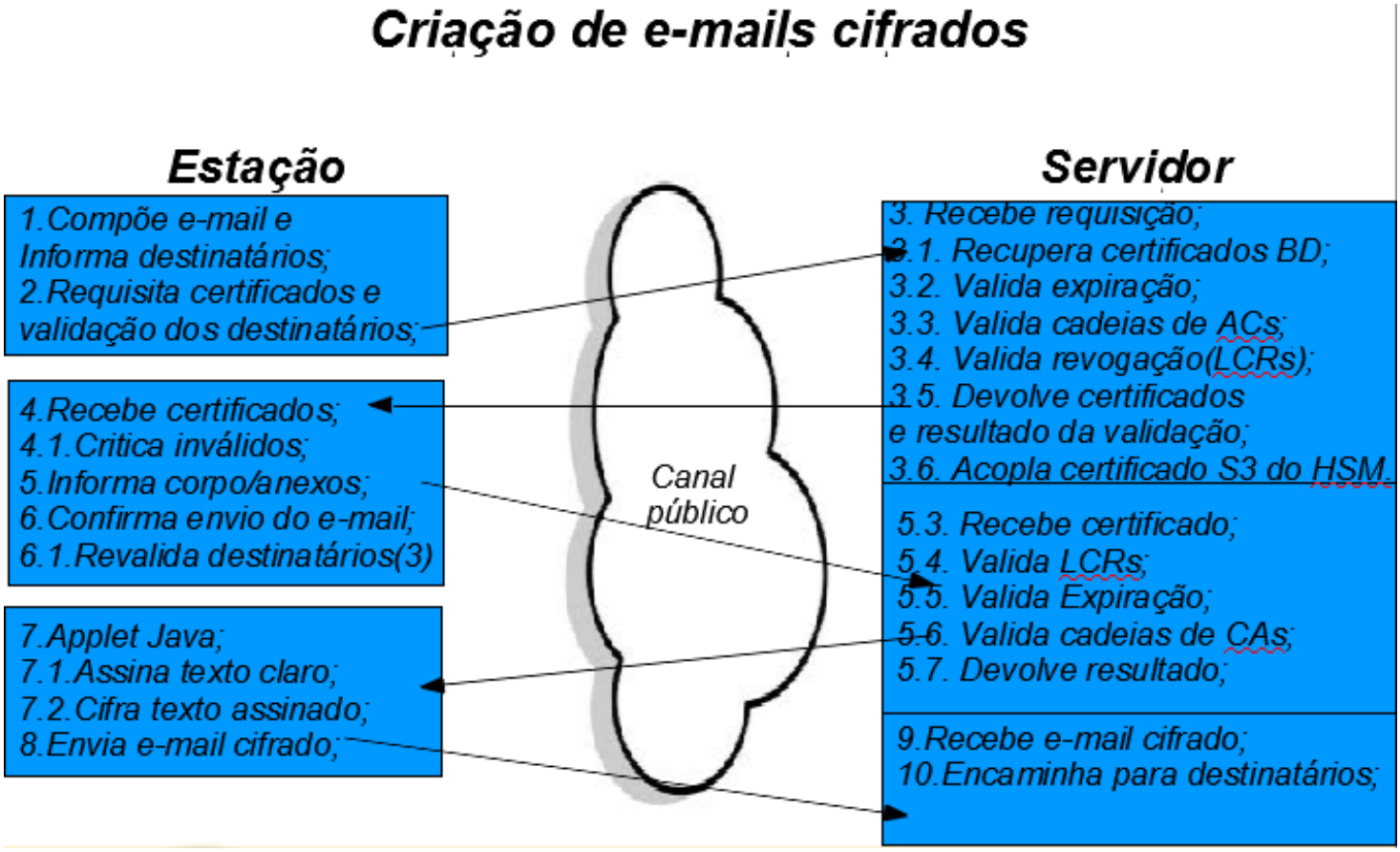

Figura 15: criação de e-mails criptografados

4.3 EXECUTANDO A AUDITORIA EM E-MAIL CRIPTOGRAFADO

Como este trabalho está sendo direcionado para correio eletrônico governamental, contudo se aplica também às empresas privadas, há norteadores em que um correio governamental tem que se pautar, um deles se dá no fato de que os programas e equipamentos que tratam sobre comunicação de dados da administração pública federal direta, autárquica e fundacional deverão ter características que permitam a auditoria, isto está preconizado no decreto presidencial nº 8.135 de 04 de novembro de 2013.

Logo, o procedimento de integração do HSM com o correio eletrônico citado no tópico acima, se faz necessário, para que nesta fase possa ser realizado a auditoria de e-mail criptografado, e que não tenha a necessidade de ter os participantes (remetente ou destinatário(s)) envolvidos no processo de quebra do sigilo da comunicação.

A primeira etapa para iniciar este processo, está em verificar a conformidade, ou seja, a necessidade de se realizar a auditoria, pois, como é um processo sigiloso e de caráter excepcional, somente em casos específicos e já mencionados é que se pode realizar tal feito.

Para isso, toda a demanda independente de ser externa ou interna, passa primeiramente pela área jurídica da empresa, com intuito desta poder avaliar se todos os critérios jurídicos foram contemplados.

Após este momento a área jurídica então encaminha a solicitação de auditoria para a equipe que administra o correio eletrônico, pois esta é a responsável por exportar a mensagem criptografada eu uma mídia óptica e levá-la ao local onde será realizada a cerimônia de auditoria.

O terceiro momento se dá na convocação dos custodiantes, sabe-se que para isso é necessário o valor “N” dos mesmos. Pode também ser chamado testemunhas, com o intuito delas apenas avaliarem o procedimento de cerimônia e atestarem que o e-mail quando for descriptografado será entregue a autoridade competente.

A validação dos custodiantes será feita pelo operador do módulo HSM, no qual é responsável por verificar as credencias de cada custodiante, verificando inclusive a autenticação dos mesmos no HSM utilizando seus Smartcards. Após a validação e autenticação, a próxima fase é de ativação da chave privada, necessária para a descriptografia.

A chave é ativada executando comando no módulo HSM para permitir que seja utilizada pelos custodiantes que ora se autenticaram, porém como não pode ser retirada do HSM, pega-se então o e-mail, coloca-o em uma estação de trabalho offline, e que esteja somente conetada ao HSM, ou seja, esta estação não tem nenhum contato com a internet, é totalmente isolada da infraestrutura da organização, e isto é necessário para garantir que em nenhum momento a máquina tenha sofrido alguma tentativa de invasão, ou tenha sido infectada por algum vírus.

Submete-se então a chave, através de uma biblioteca OpenSSL rodando na estação de trabalho, para que esta possa efetuar a descriptografia, pois como a mensagem foi criptografada também com o certificado de sigilo que contém a chave pública do HSM, logo com a utilização da chave privada, a descriptografia é realizada.

Com isso, é então retirada a criptografia e o e-mail volta a sua forma de texto original, ou seja, e-mail legível.

Dentro da mesma estação de trabalho e de posse da mensagem original, esta é convertida para formato. PDF – este formato de arquivo é utilizado para exibir e

compartilhar documentos de maneira compatível, independentemente de software, hardware ou sistema operacional, não sendo possível a sua edição – e para assegurar a legitimidade os custodiantes a assinam digitalmente.

A mensagem agora é novamente gravada numa mídia óptica e entregue a autoridade competente, ou seja, ao demandante do processo de auditoria, se for externo, através de representante legal da empresa, e se for interno, ao chefe do setor demandante.

Por fim, é importante que haja a sanitização do arquivo de e-mail que ficou na estação de trabalho, isto significa que haverá o procedimento de limpeza de disco onde este arquivo se encontra, a fim de apagá-lo de forma permanente da máquina.

Dar-se-á então o encerramento da cerimônia.

5. CONCLUSÃO

O objetivo deste trabalho foi mostrar como é possível auditar mensagens criptografadas dentro de um ambiente de correio eletrônico, mesmo que não tenha as chaves criptográficas dos participantes desta troca de mensagem.

Esta necessidade se deu no âmbito governamental principalmente ao fato de que o decreto presidencial nº 8.135 de 04 novembro de 2014, determina que a administração pública federal direta, autárquica e fundacional devem utilizar as redes de telecomunicações e serviços de tecnologia da informação, provenientes da própria administração, incluindo empresas públicas e sociedades da economia mista da União, e que ao utilizar programas e equipamentos fornecidos por estas empresas públicas, estes deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações.

Com base nisto foi proposto então, uma solução em que se utiliza o módulo criptográfico de segurança, que é um equipamento de segurança física no qual, provê diversos mecanismos de proteção, incluindo a geração e guarda de chaves privadas e públicas, integrando com o sistema de correio eletrônico.

Esta solução foi possível de ser concebida e adotada, porque há mecanismo de geração de certificado de sigilo criado dentro do módulo criptográfico, utilizando para isso um processo reconhecido como “cerimônia”, nas quais determinadas pessoas conhecidas como “custodiantes”, executam um procedimento rigoroso para que seja realizado esta geração de certificado.

Este certificado, é inserido dentro do ambiente de correio eletrônico, para que quando um usuário desejar criar um e-mail criptografado, este seja criado com o

certificado de sigilo provido pelo HSM, conjuntamente com o certificado de sigilo do destinatário.

Com isto a funcionalidade de auditoria pode ser realizado a contento, pois através deste certificado, pode-se então convocar os “custodiantes” para que realizem a quebra da mensagem criptografada, já que estes são os detentores das chaves privadas e públicas (utilizada aqui para criação do certificado de sigilo).

Percebe-se então que estando de acordo com o decreto e reconhecendo a necessidade de ter algum mecanismo em que possa quebrar o sigilo de um e-mail, quando este for criptografado, esta forma de solução se mostra muito eficaz e de uma complexidade não tão grande, fazendo com que sua aplicabilidade se dê em qualquer organização que necessite de ter tal funcionalidade.

Espera-se que este trabalho possa contribuir para a segurança da informação, e mais ainda para a auditoria das informações que estão sob guarda de mecanismos da tecnologia da informação, bem como, trazer maiores ganhos procedimentais e tecnológicos para os serviços governamentais.

Vale salientar que hoje, esta solução está em processo de finalização dentro da empresa, faltando apenas a conclusão de uma norma na qual descreve o procedimento de validação jurídica quando se tem uma demanda para realizar o processo de descriptografia, porém todo processo aqui retratado foi aplicado e está sendo realizado.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 11515** – Guia de práticas para segurança física relativa ao armazenamento de dados. 2 ed. Rio de Janeiro: ABNT, 2007.

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 15247** – Unidades de armazenagem segura - Salas cofre e cofres para hardware - Classificação e método de ensaio de resistência ao fogo. Rio de Janeiro: ABNT, 2004.

ATTIE, William. ***Auditoria – conceitos e aplicações***. 3ª ed. São Paulo. Atlas, 2000.

BRASIL, ***Instrução Normativa nº 03 do Gabinete de Segurança Institucional da Presidência da República.*** Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos. Disponível em: <http://dsic.planalto.gov.br/documentos/instrucao_normativa_nr3.pdf> Acesso em: 24 fev. 2016

BENETI, Marcos Antonio. ***Segurança e Auditoria de Sistemas.*** Disponível em: <http://www.benetti.eti.br/home/informatica/auditoria> Acesso em: 26 jan. 2016

BRASIL. **Decreto nº. 8.135**, de 4 de novembro de 2013. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-

2014/2013/Decreto/D8135.htm>. Acesso em 22 set. 2015.

BRASIL. Medida Provisória 2.200-2. **Medida Provisória que instituiu a ICPBrasil.** Disponível em: <http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm>. Acesso em: 02 mar. 2016

BURNETT, Steve. ***Criptografia e Segurança, o Guia Oficial RSA.*** 3 ed. Rio de Janeiro. Campus, 2002

CERT.BR. ***Cartilha de Segurança para Internet.*** Disponível em: <http://cartilha.cert.br>.
Acesso em: 09 dez. 2015.

COFRE DIGITAL. Disponível em: <https://www.serpro.gov.br/tema/noticias-tema/um-cofre-digital> Acesso em: 01 fev. 2016

EMILIANO S., MONTEIRO M. E. **Certificados Digitais.** 1 ed. BRASPORT. Rio de Janeiro, 2007

ICP Brasil – Infra-Estrutura de Chaves Públicas Brasileiras. **Definições do glossário**.
Brasília: Presidência da República. Disponível em: <https://www.icpbrasil.gov.br/duvidas/glossary/criptografia?searchterm=criptografia>. Acesso em: 17 jan. 2016

ICP Brasil - ***Manual de Condutas Técnicas 7 – Volume I: Requisitos, Materiais e Documentos Técnicos para Homologação de Módulos de Segurança Criptográfica MSC) no Âmbito da ICP-Brasil.*** Disponível em http://www.iti.gov.br/noticias/132-servicos/homologacoes/1360-manuais-de-condutas-tecnicas-mct-s Acesso em: 04 out. 2015

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO – ***CERTIFICADO DIGITAL*** Disponível em: http://www.iti.gov.br/certificacao-digital/certificado-digital Acesso em: 29 nov. 2015

GRASSELLI, Oraci Maria. ***Internet, Correio Eletrônico e Intimidade do Trabalhador.*** 1 ed. São Paulo. LTR, 2011

HOUAISS, Antonio. **Dicionário Eletrônico Houaiss da Língua Portuguesa**. 2. ed. São Paulo: Ed. Objetiva, 2009.

HOUSLEY, Russ. *P**lanning for PKI: Best Practices Guide for Deploying Public Key Infrastructure*.** Wiley, 2014.

HSM Kryptus - ***Especificação técnica módulo de segurança criptográfico***. Disponível em: http://www.kryptus.com/#!asi-hsm/c11e6 Acesso em: 03 set. 2015

LOUREIRO, César Augusto Hass. ***Redes de Computadores - Nível de aplicação e instalação de serviços.*** Bookman, 2013

MANUEL, P. ***A Função Auditoria de Sistemas de Informação: Modelo Funcional e de Competências.*** Braga, 2007

NIST **National Institute of Standards and Technology**, PKI Project Team, Certificate Issuing and Management Components Protection Profile. National Security Agency, USA, 2002.

NUNES, Délio Silva. ***PKI – Public Key Infrastructure***. Disponível em: <http://www.gta.ufrj.br/grad/07_2/delio/ICP-Brasil.html> Acesso em dia 09 fev. 2016

PC Magazine. ***PCMAG.COM Encyclopedia – Definition cryptography***. EUA. Disponível em: <http://www.pcmag.com/encyclopedia_term/0,2542,t=cryptography&i=40522,00.asp> Acesso em: 07 jan. 2016

PKI Consulting – ***Nota do ITI sobre Uso do HSM***. Disponível em: http://www.pkiconsulting.com/blog/nota-do-iti-sobre-uso-de-hsm Acesso em 26 set. 2015

SALGADO, Hugo David Marques. ***Código Morse: O que é e como surgiu***. Disponível em: <https://student.dei.uc.pt/~hsalgado/CP/artigo.htm> Acesso em: 05 fev. 2016

SCHIMITT, Marcelo Augusto Rauh. ***CRIPTOGRAFIA DE CHAVES PÚBLICAS - RNP (Rede Nacional de Ensino e Pesquisa).*** Disponível em :

<http://www.rnp.br/wrnp2/2001/palestras_middleware/pal_middl_02.pdf > Acesso em: 04 mar. 2016

SCHNEIER, Bruce. **Applied Cryptography – Protocols, Algorithms, and Source Code in C**. 2 ed. New York: John Wiley & Sons, Inc., 2003.

SINGH, Simon – ***The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*.** Paperback, 2000.

STALLINGS, William. **Cryptography and Network Security – Principles and Practices.**4 ed. New Jersey, EUA: Prentice Hall, 2008.

WIKIPEDIA, a Enciclopédia Livre - ***Técnica Secret Sharing*.** Disponível em: http://en.wikipedia.org/wiki/Secret_sharing Acesso em: 09 out. 2015

NIST FIPS PUB 140-2 Security Requirements For Cryptographic Modules

YOSHIDA, Elias Yoshiaki - MAC 39, Informação, Comunidade e a Sociedade do Conhecimento. Disponível em: <https://www.ime.usp.br/~is/ddt/mac339/projetos/2001/demais/elias/> Acesso em: 15 jan. 2016

ANEXO

DECRETO Nº 8.135, DE 4 DE NOVEMBRO DE 2013

A PRESIDENTA DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, **caput**, inciso IV, da Constituição, e tendo em vista o disposto no art. 24, **caput**, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, ouvido o Conselho de Defesa Nacional.

DECRETA:

Art. 1º As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias.

§ 1º O disposto no **caput** não se aplica às comunicações realizadas através de serviço móvel pessoal e serviço telefônico fixo comutado.

§ 2º Os órgãos e entidades da União a que se refere o **caput** deverão adotar os serviços de correio eletrônico e suas funcionalidades complementares oferecidos por órgãos e entidades da administração pública federal.

§ 3º Os programas e equipamentos destinados às atividades de que trata o **caput** deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, na forma da regulamentação de que trata o § 5º.

§ 4º O armazenamento e a recuperação de dados a que se refere o **caput** deverá ser realizada em centro de processamento de dados fornecido por órgãos e

entidades da administração pública federal.

§ 5º Ato conjunto dos Ministros de Estado da Defesa, do Planejamento, Orçamento e Gestão e das Comunicações disciplinará o disposto neste artigo e estabelecerá procedimentos, abrangência e prazos de implementação, considerando:

I - as peculiaridades das comunicações dos órgãos e entidades da administração pública federal; e

II - a capacidade dos órgãos e entidades da administração pública federal de ofertar satisfatoriamente as redes e os serviços a que se refere o **caput**.

Art. 2º Com vistas à preservação da segurança nacional, fica dispensada a licitação para a contratação de órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, para atendimento ao disposto no art. 1º.

§ 1º Enquadra-se no **caput** a implementação e a operação de redes de telecomunicações e de serviços de tecnologia da informação, em especial à garantia da inviolabilidade das comunicações de dados da administração pública federal direta e indireta.

§ 2º Os fornecimentos referidos no § 1º para a administração pública federal consistirão em:

I - rede de telecomunicações - provimento de serviços de telecomunicações, de tecnologia da informação, de valor adicionado e de infraestrutura para redes de comunicação de dados; e

II - serviços de tecnologia da informação - provimento de serviços de desenvolvimento, implantação, manutenção, armazenamento e recuperação de dados e operação de sistemas de informação, projeto de infraestrutura de redes de

comunicação de dados, modelagem de processos e assessoramento técnico, necessários à gestão da segurança da informação e das comunicações.

§ 3º A dispensa de licitação será justificada quanto ao preço pelo órgão ou entidade competente pela contratação.

Art. 3º Este Decreto entra em vigor:

I - na data de sua publicação, em relação ao art. 2º; e

II - em cento e vinte dias após a data de sua publicação, em relação ao art. 1º.

Brasília, 4 de novembro de 2013; 192º da Independência e 125º da República.

DILMA ROUSSEFF

Celso Luiz Nunes Amorim

Miriam Belchior

Paulo Bernardo Silva