UNIVERSIDADE DA FORÇA AÉREA BRASILEIRA

MESTRADO EM CIÊNCIAS AEROESPACIAIS

LUIZ CLÁUDIO FONSECA DE MOURA

INFRAESTRUTURA DE CHAVES PÚBLICAS NO COMANDO DA AERONÁUTICA

RIO DE JANEIRO
Dezembro 2010

LUIZ CLÁUDIO FONSECA DE MOURA

INFRAESTRUTURA DE CHAVES PÚBLICAS NO COMANDO DA AERONÁUTICA

Dissertação apresentada como requisito parcial para a obtenção do título de Mestre em Ciências Aeroespaciais pela Universidade da Força Aérea (UNIFA).

ORIENTADOR: PROF. DR. AMÂNDIO MARQUES DA COSTA JÚNIOR (UGF)

RIO DE JANEIRO
Dezembro 2010

RESUMO

Com o avanço tecnológico, a dependência por sistemas informatizados vem aumentando. Para garantir a segurança destes sistemas, foi desenvolvida a Teoria de Segurança das Informações. Um dos modelos estudados nesta Teoria é a certificação digital, baseada na criptografia de chaves assimétricas. O COMAER, seguindo normas rígidas do Governo, bem como, a tendência mundial, desenvolveu sua própria assinatura digital, oriunda de sua infraestrutura de chaves públicas. Este estudo pretendeu analisar *o processo de certificação digital na segurança das atividades de TI no âmbito* do Comando da Aeronáutica. Para isto, este trabalho fez uso de uma extensa pesquisa bibliográfica, tendo como base a medida Provisória n° 2200-2, de 24 de agosto de 2001, que institui a Infraestrutura de Chaves Públicas Brasileira e as normas e legislações do Instituto Nacional de Tecnologia da Informação. A fim de dar embasamento teórico ao diagnóstico utilizou-se a Teoria Geral de Administração bem como a Teoria da Criptografia, encontrada em obras de autores como Idalberto Chiavenato, em seu livro Introdução à Teoria Geral da Administração, e no livro Segurança de dados: Criptografia em redes de computadores do professor da USP, Routo Terada. Utilizou-se ainda de pesquisa documental em publicações internas do COMAER, alicerçada em uma pesquisa de campo *on line* com respostas objetivas e outra com perguntas discursivas em um formulário. Constatou-se que a infraestrutura de chaves do COMAER atende aos requisitos de normatização do Governo Brasileiro e que, em breve, poderá proporcionar uma sensível melhoria, agilidade e segurança nos processos administrativos da instituição Verificou-se também que na área militar, o COMAER é a única instituição que detém o conhecimento completo e a infraestrutura quase pronta para o funcionamento no país. Conclui-se que a certificação digital do COMAER acompanha o que há de mais moderno no conceito mundial, e que em breve, proporcionará à instituição uma enorme mudança cultural administrativa e operacional ao imprimir agilidade, segurança, integridade e autenticidade ao trâmite das informações institucionais disponibilizadas eletronicamente, sendo reconhecido como um projeto viável e importante para a Comando. Os dados estão atualizados até dezembro de 2010.

Palavras-chave: Assinatura digital. Segurança da Informação. Tecnologia da Informação. Criptografia.

ABSTRACT

With the technological advancement, the dependence on computer systems is increasing. To ensure the safety of these systems the Theory of Information Security was developed. One of the models studied in this Theory is the digital certification, based on cryptography of asymmetric keys. The COMAER, following strict standards from the Government, as well as, the worldwide trend, has developed its own digital signature, from its infrastructure of public keys. This study aimed to analyze the process of digital certification in the safety of the activities of TI under the command of the Air Force. For this, this work has made use of an extensive bibliographic research and on the basis of the Provisional measure n ° 2200-2, August 24, 2001, establishing the Infrastructure of Brazilian Public Keys and the standards and laws of the National Institute of Information Technology. In order to give theoretical background to the diagnosis, the General Theory of Administration was used as well as the Theory of Cryptography, found in works of authors such as Idalberto Chiavenato, in his book Introduction to the General Theory of the Administration, and in the book Data Security: Cryptography in computer networks of the professor of USP, Routo Terada. We also used documental research of internal publications of COMAER, grounded in a field research on line with objective answers and another with discursive questions in a form. It was noted that the infrastructure of keys of COMAER complies with the requirements for standardization of the Brazilian Government and that, soon, can provide a clear improvement, agility and safety in the administrative processes of the institution. It was also noted that in the military field, the COMAER is the only institution that holds the complete knowledge and infrastructure almost ready for the operation in the country. We conclude that the digital certification of COMAER accompanies the most modern in worldwide concept, and that in the near future, it will give the institution a huge administrative change cultural and operational when engraving speed, security, integrity and authenticity to the formality of institutional information available electronically, being recognized as a feasible project and important to the Comand. The data are updated up to December 2010.

Keywords: Digital Signature. Information Security. Information Technology. Encryption.

LISTA DE ABREVIATURAS E SIGLAS

AC	- Autoridade Certificadora
AR	- Autoridade de Registro
BSI	- *Bundesamt für Sicherheit in der Informationstechnik*[1]
CAB	- Comissão Aeronáutica Brasileira
CABW	- Comissão Aeronáutica Brasileira em *Washington*
CASNAV	- Centro de Análises de Sistemas Navais
CCABR	- Centro de Computação da Aeronáutica de Brasília
CCEM	- Curso de Comando e Estado-Maior
CG	- Comitê Gestor
CDS	- Centro de Desenvolvimento de Sistemas
COMAER	- Comando da Aeronáutica
COMPRASNET	- Sistema de compras via *Internet*
COTEC	- Comissão de Assessoramento Técnico
DECEA	- Departamento de Controle do Espaço Aéreo
DIRAP	- Diretoria de Administração de Pessoal
DIRINT	- Diretoria de intendência
DIRSA	- Diretoria de Saúde
DPC	- Declaração de Práticas de Certificação
ECEMAR	- Escola de Comando e Estado- Maior da Aeronáutica
EUA	- Estados Unidos da América
FBCA	- *US Government´s Federal Bridge Certification Authority*
ICP	- Infraestrutura de Chaves Públicas
INTRAER	- Rede corporativa do Comando da Aeronáutica

[1] *Bundesamt für Sicherheit in der Informationstechnik* (BSI) - Agência governamental de segurança da informação.

INTRANET	- Rede corporativa
INTERNET	- Rede mundial de computadores
I/O	- *Input/Output*
IuKDG	- *Informations- und Kommunikationsdienste- Gesetz*[2]
ITI	- Instituto Nacional de Tecnologia da Informação
LAN	- *Local Área Network*
MD	- Ministério da Defesa
MD5	- *Message Digest five*
OM	- Organização Militar
OS	- Organizações de Saúde da Aeronáutica
PC	- Política de Certificação
PIB	- Produto Interno Bruto
PKI	- *Public Key Infrastructures*
PIN	- *Personal Identification Number*
PSS	- Prestadores de Serviço de Suporte
ReGT	- *Regulierungsbehoerde für Telekommunikation und Post*[3]
RIC	- Registro de Identificação Civil
ROM	- *Read Only Memory*
RFID	- *Radio-Frequency Identification*
SDAB	- Subdiretoria de Abastecimento
SDPP	- Subdiretoria de Pagamento de Pessoal
SEFA	- Secretaria de Finanças da Aeronáutica

[2] *Informations- und Kommunikationsdienste- Gesetz (IuKDG)* - lei de serviços de informação e comunicação, superior a SigG define as diretrizes da certificação digital na Alemanha.

[3] *Regulierungsbehoerde für Telekommunikation und Post* (ReGT) - Agência Reguladora para Telecomunicação e Correios (autoridade certificadora raiz).

SERPRO - Serviço Federal de Processamento de Dados

SHA - *Secure Hash Algorithm*

SIAFE - Sistema Integrado de Administração Financeira do Gov. Federal

SIAPE - Sistema Integrado de Administração de Pessoal

SigG - *Lei Signaturgesetz*[4]

SIDENT - Sistema de Identificação Civil

SIGPES - Sistema de Informações Gerenciais de Pessoal

SIORG - Sistema de Informações Organizacionais do Governo Federal

SSL - *Secure Socket Layer*

STI - Sistema de Tecnologia da Informação

UAe - Unidade Aérea

VPN - *Virtual Private Network*

WAN - *Wide Area Network*

[4] *Signaturgesetz* (SigG) - lei subsidiária da lei IuKDG, define as normas de certificação digital no pais.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ANEXOS

SUMÁRIO

1 INTRODUÇÃO

1.1 CONCEITOS GERAIS

A informação tem se constituído em uma importante ferramenta nas relações entre os seres humanos. O desenvolvimento dos meios computacionais, cuja sofisticação atingiu elevados níveis na sociedade atual, permitiu a implementação do trâmite de informações em tempo real, por meio de redes de transporte de dados, como a rede de dados mundial (*Internet*) e das redes de dados corporativas (*intranet*).

Essa expansão do mundo digital aponta a existência de uma revolução de comportamento social no mundo moderno, proporcionando o surgimento da chamada Sociedade da Informação.

O crescimento contínuo e ininterrupto desta sociedade, aliado ao desenvolvimento da Tecnologia da Informação (TI) nas diversas instituições públicas e privadas, proporcionado pela evolução computacional, deu origem a um dos principais focos da sociedade da informação, a segurança; dessa forma, essa sociedade se depara com a necessidade de soluções que proporcionem ao homem moderno a garantia dos quesitos de inviolabilidade, integridade e autenticidade a todo o trâmite de informações institucionais e pessoais disponibilizadas eletronicamente via rede.

O paradigma que emerge dessa revolução é a prevalência da informação eletrônica, gerando um conjunto de novas relações econômicas e sociais, vivenciadas pela sociedade de maneira cada vez mais natural. Esse conjunto de transações eletrônicas, denominado negócios eletrônicos – "*e-business*", ocorre entre os diversos setores da sociedade, quer sejam empresas, cidadãos e governo.

Neste sentido, surgem programas e atividades essenciais visando orientar e treinar o homem moderno no que se refere aos cuidados que devem adotar no manuseio de informações digitais.

A implementação apropriada de uma política de segurança da informação deverá atender por completo aos requisitos de segurança, tornando a informação

detentora de todos atributos necessários a sua utilização de forma ampla e confiável. Uma das soluções tecnológicas mais utilizadas atualmente, disseminada pelo uso de redes de computadores, é a criptografia. No entanto, segundo a Câmara Brasileira de Comércio Eletrônico em sua cartilha sobre certificação digital, “[...]a utilização de métodos criptográficos distintos, sem gerenciamento, nem padrões específicos, ao invés de agilizar os negócios eletrônicos, pode até resultar na sua inviabilização”.

O crescente interesse mundial por aumento da segurança no trâmite de informações despertou no Governo Brasileiro uma busca por soluções confiáveis pautadas por normas bem definidas. Foi assim que surgiu no contexto brasileiro o Comitê Gestor de Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil) e o Instituto Nacional de Tecnologia da Informação (ITI), autarquia federal vinculada à Casa Civil da Presidência da República.

O ITI tornou-se a primeira autoridade da cadeia de certificação, possuindo como atribuição executar as Políticas de Certificados e normas técnicas operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.

Tal entidade foi criada para ser a Autoridade Certificadora Raiz - AC Raiz da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, sendo responsável por emitir, expedir, distribuir, revogar e gerenciar os certificados das Autoridades Certificadoras - AC de nível imediatamente subsequente ao seu, bem como, estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital.

Dentro da esfera militar, não só surgiu a determinação por parte do Governo Brasileiro para adequação de todos seus órgãos ao ingresso na rede de alta velocidade conectada aos órgãos intergovernamentais (INFOVIA), como também, a necessidade do Ministério da Defesa (MD) e dos Comandos da Marinha, Exército e Aeronáutica, de implementação desta nova tecnologia viabilizando segurança, economia e agilidade no trâmite de informações.

1.2 JUSTIFICATIVA

Em função da importância do assunto, bem como, da necessidade do domínio desta tecnologia por parte do Comando da Aeronáutica (COMAER), o Departamento de Controle do Espaço Aéreo (DECEA), em meados de 2003, designou o Centro de Computação de Aeronáutica de Brasília (CCABR) para o desenvolvimento do projeto da Autoridade Certificadora do Comando da Aeronáutica (AC-COMAER). Naquela ocasião o autor desse trabalho prestava serviço no referido Centro de Computação.

Paralelo a isso, deu-se início ao projeto da autoridade certificadora da Marinha designado “Projeto João de Barro”; por meio do Centro de Análise de Sistemas Navais (CASNAV). Da mesma forma, no Comando do Exército, o Centro de Desenvolvimento de Sistemas (CDS) iniciava o projeto da AC daquela Força.

O assunto torna-se de importância, não só para o Comando da Aeronáutica, mas também para o Ministério da Defesa (MD), por se tratar de uma inovação tecnológica que poderá ser utilizada nas seguintes situações:

a) na administração interna;
b) nas operações militares;
c) nas ordens de missões;
d) nos trâmites de *e-mail;*
e) nos documentos da Força;
f) na elaboração de boletins internos e externos;
g) nas assinaturas de contratos;
h) na validação de contracheque pela Internet, e
i) no acesso a rede interna por militares no exterior, dentre outras possíveis alternativas a serem identificadas no futuro.

Além das citadas anteriormente, poderá proporcionar segurança, economia e agilidade em diversas outras situações.

Com a experiência de oito anos servindo no Centro de Computação da Aeronáutica de Brasília, o tema proposto foi resultado da observação contínua, e do trabalho do autor na implementação da estrutura de chave pública do COMAER,

sendo necessário para isso a participação em diversos cursos, seminários e palestras, com o intuito de aprofundamento no assunto por se tratar de algo pouco conhecido no país.

Visando elucidar o seguinte problema: “Como a certificação digital pode otimizar as atividades administrativas do Comando da Aeronáutica?” O presente trabalho propõe enfocar a certificação digital dentro da Aeronáutica, bem como a sua utilização na moderna administração da Força.

Afim de orientar a condução deste trabalho, as seguintes questões norteadoras serão utilizadas para a execução desta dissertação: o que é a certificação digital; o que é criptografia de chaves assimétricas e assinatura digital; qual é a estrutura reguladora da certificação digital; quais são as diferenças entre o modelo brasileiro e o de outros países; quais são as vantagens para a Força Aérea.

Desta forma é possível observar que trata-se de um tema bastante oportuno na atualidade, por ser um assunto novo no contexto mundial e extremamente interessante para a otimização administrativa de qualquer tipo de organização. Ressalta-se que a necessidade demandada pela sociedade da informação, por segurança de dados transmitidos através das redes, por si, expressa a relevância do assunto.

1.3 OBJETIVOS

Por se tratar de um tema que alia tecnologia e formalismo legal, é que o objetivo desse trabalho, consiste em analisar *o processo de certificação digital na segurança das atividades administrativas no âmbito* do Comando da Aeronáutica, trazendo uma abordagem introdutória ao tema, contribuindo para o entendimento do assunto, dos seus aspectos, das vantagens da sua utilização e da desburocratização das atividades administrativas do COMAER.

Com isso, alguns objetivos específicos serão necessários e norteadores desta dissertação:

a) Levantar os conceitos de certificação digital no mundo contemporâneo.

Ao alcançar este objetivo, ter-se-á condições de se identificar a definição e o significado da certificação digital e como pode prover a segurança da informação.

b) analisar os tipos de criptografia;

Ao atingir este objetivo, serão esclarecidos os tipos de criptografias existentes e o modelo adotado para utilização na certificação digital.

c) Identificar a estrutura reguladora de certificação digital no Brasil?;

Com este passo, poder-se-á entender como a teoria da burocratização contribui para estabelecer a infraestrutura de chaves públicas brasileiras bem como conhecer as documentações que normatizam sua estrutura.

d) efetuar uma análise comparativa sobre a utilização da certificação digital em outros países; e

Após este tópico o leitor poderá ter uma comparação da estrutura de certificação utilizada no Brasil, seu modelo e a comparação com outros países.

e) verificar a utilização da certificação nas instituições brasileiras e as vantagens que poderão ser agregadas ao COMAER.

Assim, sendo atingido cada objetivo listado anteriormente é que se poderá, por meio de uma analogia, apontar as possíveis vantagens da utilização da certificação digital dentro do COMAER.

1.4 ESCOPO DO TRABALHO

A certificação digital traz consigo um marco regulador e está pautada na teoria da criptografia e amparada por uma infraestrutura de chaves públicas. Essa situação não poderia ser diferente, uma vez que, quando se trata de certificação digital, o binômio segurança e legalidade caminham juntos.

Com base na teoria clássica da administração, caracterizada pela ênfase na estrutura que a organização deve possuir para ser eficiente (Fayol), a certificação digital promove algo de novo em uma instituição baseada em hierarquia e burocratização.

A estrutura legal de uma instituição deve ser planejada para acompanhar os costumes presentes em sua evolução temporal trazida pela tecnologia. Assim, a certificação digital surge como uma novidade que deve ser compreendida. Ela veio como algo que chega para fortalecer preceitos difundidos e enraizados na estrutura organizacional, a “Teoria da burocratização” de Max Weber.

Indo um pouco mais além, define Fayol: “O ato de administrar é: prever, visualizar o futuro e traçar o programa de ação; organizar, constituir o duplo organismo matricial e social da empresa;...” (CHIAVENATO, 2001, p. 93).

Dentre essas funções, prever, visualizar o futuro e traçar programas de ação são atividades inerentes ao administrador diante das soluções tecnológicas dos nossos dias. Desta forma, pode-se extrair uma visão que resume o contexto em que se vive atualmente, qual seja: o da criptografia na era da informação segura, inserida nas teorias clássicas da administração, dando origem a estrutura da moderna organização administrava das instituições.

Para facilitar a compreensão o trabalho aborda no primeiro capítulo a importância do assunto no contexto nacional e no âmbito militar. Em seguida, no segundo são apresentados os tipos de criptografia e o mecanismo de assinatura digital, bem como uma explicação do que vem a ser a certificação digital. No terceiro capítulo capítulo, é apresentado a estrutura reguladora da certificação digital no Brasil, uma comparação entre modelos de certificação de outros países, a certificação digital na Força e as vantagens que poderão ser agregadas ao COMAER. Em seguida no quarto capítulo estabelece-se a metodologia cientifica utilizada e por fim conclui-se o trabalho apresentando os resultados encontrados e sugestões para o futuro.

Estabelecidos os conceitos gerais necessários ao entendimento do tema, sua importância, os objetivos que se pretende atingir e o escopo do trabalho, cabe agora abordar a segurança de dados e a criptografia digital no mundo contemporâneo.

2 UMA VISÃO DA SEGURANÇA DE DADOS E CERTIFICAÇÃO DIGITAL NO MUNDO COMTEPORÂNEO

A utilização de meios computacionais para melhor gerir complexos sistemas de informação é uma preocupação latente em todas as grandes organizações do mundo globalizado. Neste contexto, possuir informações e saber como tratar essas informações é um grande diferencial competitivo.

Há tempos os homens utilizam assinaturas à caneta, carimbos e selos para comprovar a autenticidade de documentos, demonstrar sua aquiescência em relação a determinados assuntos, bem como eximir-se ou aceitar certas responsabilidades perante o Estado.

Hoje, já é factível que todas essas atividades sejam feitas por meio do uso da Internet. Mas, como garantir autenticidade, expressar concordância ou declarar responsabilidade no "mundo digital"? É aí que entra em cena a **certificação digital** e seus conceitos relacionados, como assinatura digital.

2.1 O QUE É CERTIFICAÇÃO DIGITAL?

Em um mundo onde a informação é traduzida em “poder”, as corporações cada vez mais estão preocupadas com o processo de certificação digital, cujo método utiliza procedimentos lógicos e matemáticos que, combinados, asseguram 04 (quatro) pilares fundamentais que sustentam a guarda e proteção da informação, são eles:

a) **integridade** - a criptografia é usada para garantir que uma informação não seja adulterada durante a transmissão ou armazenamento. Qualquer pessoa pode ter acesso ao conteúdo da informação, porém ninguém poderá alterá-la;

b) **autenticidade** - a criptografia é usada para identificar uma pessoa através de uma transação remota. Aqui pode-se fazer um paralelo com o mundo real. Quando se faz uma compra em uma loja, o caixa solicita que o comprador apresente seus documentos de identificação

para que ele possa ter certeza de que a pessoa é realmente quem diz ser. Ela faz isso através de uma identificação visual ou mesmo da confrontação da assinatura da pessoa.

Quando se fala de transações remotas através da rede, não existe contato físico tornando ineficaz qualquer tipo de identificação pelos métodos tradicionais. Existe indefinição entre os autores quanto ao conceito de autenticação. Alguns colocam a autenticação e a certificação como tendo o mesmo significado. Optou-se nesse texto por duas definições distintas por se entender que, apesar de aplicarem mecanismos criptográficos idênticos, os resultados alcançados são distintos.

Entende-se nesse texto como autenticação, o processo puro e simples de identificar uma pessoa através da rede, porém sem gerar nenhum tipo de prova do procedimento. É como quando o caixa, de posse da identidade do comprador, analisa o documento, confronta a fotografia e se dá por satisfeito entendendo ter identificado a pessoa. Na rede, isso se faz através de um desafio. A pessoa que deseja identificar a outra lança um desafio que ela tem certeza que somente quem poderá respondê-lo corretamente é a pessoa com quem ela acredita que está falando. Quando chega a resposta do desafio ela verifica se a resposta está correta. Se estiver, dá-se por satisfeita e continua a transação tendo certeza de com quem ela está falando. Porém, esse processo não gera nenhuma prova da transação, é apenas um processo de identificação;

c) **sigilo** – a criptografia é usada para garantir o conteúdo de uma informação sendo negado o seu teor a qualquer pessoa não autorizada; e
d) **irrefutabilidade** – a criptografia é utilizada para gerar provas de que aquele arquivo, imagem ou assinatura é fidedigna e irrefutável.

A tecnologia atualmente empregada no mundo para prover esses quatro pilares é denominada Infraestrutura de Chaves Públicas (ICP).

Alinhando as tendências mundiais, o governo brasileiro tem envidado esforços para adoção da governança de uma política eletrônica com a finalidade de aprimorar o seu modelo de gestão.

Entende-se como governança de política eletrônica o conjunto de ações da administração pública voltadas para cidadãos, que tem por objetivo prover uma articulação entre os recursos da tecnologia da informação e os processos governamentais, proporcionando uma mediação eletrônica entre Estado e cidadão.

Com a intenção de garantir a identificação mútua entre Estado e cidadão, o Governo Brasileiro adotou a criação de uma Infraestrutura de chaves públicas (ICP). Essa ICP provê a geração e distribuição de arquivos eletrônicos, chamados Certificados Digitais:

> Um certificado digital é um arquivo de computador que contém um conjunto de informações referentes à entidade para o qual o certificado foi emitido (seja uma empresa, pessoa física ou computador) mais a chave pública referente à chave privada que acredita-se ser de posse unicamente da entidade especificada no certificado.[5]

No âmago da certificação digital está inserido o certificado digital, um arquivo eletrônico que contém as informações necessárias para identificar, com precisão e segurança, um número público exclusivo denominado chave pública, além de outros dados que mostram quem somos para as pessoas e para os sistemas de informação.

Os Certificados Digitais possuem como fim precípuo o de associar uma entidade, pessoa física, jurídica ou equipamento a um processo matemático/computacional, tendo como moderador um terceiro agente confiável representando o Estado brasileiro e denominado Autoridade Certificadora.

Na prática, o Certificado Digital funciona como uma carteira de identidade virtual, que possui fé pública e validade jurídica, permitindo transações legais entre entidades em meio digital.

A certificação digital é a tecnologia que provê todos esses mecanismos e permite, ao seu possuidor, fazer uso de uma assinatura digital com responsabilidade legal.

Para que fosse possível viabilizar a proposta de Infraestruturas de Chaves Públicas, respeitando e cumprindo os princípios da integridade, autenticidade e não

---

[5]SILVA, Lino Sarlo da. *Public Key Infrastructure PKI*. 1 ed. São Paulo: Novatec, 2004.

repúdio, desenvolveu-se o método de chaves assimétricas, que será apresentada no capítulo a seguir.

2.2 CRIPTOGRAFIA DE CHAVES

A criptografia é tão antiga quanto a própria escrita. Já estava presente no sistema hieroglífico dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalha.

> Criptografia (kriptós = escondido, oculto; grápho = grafia) : é a arte ou ciência de escrever em cifra ou em códigos, de forma a permitir que somente o destinatário a decifre e compreenda. (http://pt.wikipedia.org/wiki, 2008).

A criptografia era usada de uma forma rudimentar por César durante o Império Romano. Para garantir que sua mensagem seria recebida de forma fidedigna pelos seus exércitos nos campos de batalha, fazia-se o uso de um artificio de codificação. Cada comandante possuía um cinturão que lhe fornecia a chave para decodificar as mensagens enviadas por César. Na realidade, tratava-se de um artificio simples porém funcional.

A mensagem original era deslocada de alguns caracteres antes de seu envio. Por exemplo: a letra “A” era representada pela letra “N”, pois a mesma estava deslocada de 13 posições no alfabeto. Cada comandante de centúria possuía seus decodificadores que eram aplicados sobre o texto recebido para obter a mensagem original de César. Estava assim implantado o conceito de chaves de mensagens.

Na figura a seguir observa-se como isso era feito.

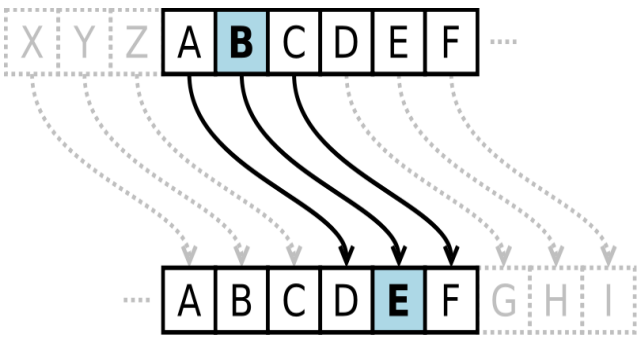


Figura 1: Criptografia de César.
Fonte: (SIPSER, Michael. Introdução à Teoria da Computação. 2. ed.).

O mais interessante é que a tecnologia de criptografia não mudou muito até meados deste século. Depois da Segunda Guerra Mundial, com a invenção do computador, a área realmente floresceu incorporando complexos algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços para decifração de códigos. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna.

Os métodos de codificação evoluíram, e continuam a evoluir, pois a informação, desde o tempo de César, já era tratada como um importante ativo capaz de definir uma vitória. No mundo da certificação digital, isso não é diferente. Por se tratar de uma estrutura na qual deve ser garantida a integridade, autenticidade, sigilo e não repúdio da origem, as questões de segurança se tornam primordiais.

Esses quatro princípios formam o núcleo legal da certificação. Para suportar esses princípios, um robusto sistema de criptografia foi proposto para todas as infraestruturas de chaves públicas do mundo, pois os meios pelos quais transitam os documentos digitais com a assinatura eletrônica dos usuários são tão ou mais inseguros do que os campos de batalha dos tempos dos Césares.

Nos dias de hoje, seria impossível disponibilizar chaves para os destinatários de todos nossos documentos enviados, mesmo por que, muitas vezes nós não os conhecemos e por vezes não temos o conhecimento prévio do destino.

Distribuir uma chave para cada recebedor de *e-mail*, por exemplo, seria algo de inimaginável para ambientes abertos ou mesmo na Internet. Ao transportar a chave com o documento eletrônico, também estaria se produzindo janelas de oportunidades para pessoas que fazem mal uso intencional de ferramentas, pois essas poderiam ser facilmente recuperadas pelos maliciosos. Seria o mesmo que pensar nos mensageiros de César transportando a chave de cifração junto com a mensagem.

2.3 TIPOS DE CRIPTOGRAFIAS

São denominados algoritmos criptográficos aqueles que implementam funções que utilizam algum tipo de criptografia para garantir sigilo, integridade e

autenticidade de uma mensagem. Os algoritmos criptográficos, basicamente, objetivam esconder informações sigilosas de qualquer agente desautorizado a lê-las, isto é, de qualquer agente que não conheça a chamada chave secreta de criptografia para decifrá-la.

Porém, é importante salientar que os algoritmos criptográficos não implementam o serviço em si, mas são instrumentos para que os serviços sejam prestados. Desta forma, um mesmo algoritmo criptográfico pode ser usado para implementar outros serviços diferentes, dependendo da forma como é usado.

2.3.1 CIFRA

São denominadas cifras todos os algoritmos criptográficos utilizados de alguma forma para garantir a confidencialidade de uma informação. As cifras, através de um processo baseado na teoria da entropia, embaralham a informação de forma organizada e disponibilizam esta informação com a possibilidade de ser desembaralhada com o auxílio de uma chave guardada em segredo.

Portanto, ao segredo usado para cifrar e decifrar dá-se o nome de chave e ao método de embaralhamento dá-se o nome de cifra.

2.3.2 CRIPTOGRAFIA SIMÉTRICA

Criptografia de chaves simétricas é aquela na qual a mesma chave de cifragem é usada para decifrar. Este tipo de criptografia possui como vantagem o desempenho e como desvantagem a distribuição da chave, ou seja, a necessidade da circulação da mesma chave que cifrou a mensagem. (Fig. 2).

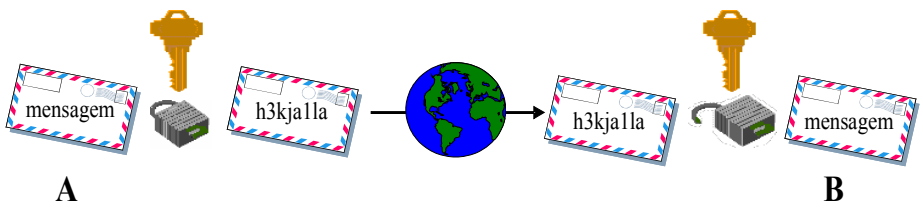


Figura 2: Criptografia de chaves simétricas.
Fonte: Autor.

2.3.3 CRIPTOGRAFIA ASSIMÉTRICA

Segundo Routo Terada em seu livro Segurança de dados a criptografia de chaves assimétricas é aquela na qual a chave utilizada para a cifragem é diferente da chave utilizada para a decifragem. Isto é, usa-se uma chave para cifrar o texto e no momento de decifrá-la usa-se outra chave que é inversa da primeira. Dessa forma, temos um par de chaves únicas e inversas entre si, não mais uma mesma chave para criptografar e descriptografar.

Costuma-se também chamar as criptografias assimétricas de criptografia de chave pública e chave privada. Isso porque normalmente uma das chaves do par é tornada pública e a outra é mantida em segredo pelo proprietário da mesma. Esse método propicia a implementação em outros modelos que não o sigilo dos dados, como nos serviços de autenticação e certificação.

Porém, é importante ressaltar que toda criptografia de chave pública é uma criptografia assimétrica, mas nem toda criptografia assimétrica é uma criptografia de chave pública.

Para que uma criptografia seja assimétrica basta que a chave de cifragem seja distinta da chave de decifragem. Porém nada garante que a partir de uma chave não se derive a outra. Uma cifra para ser reconhecida como par de chaves pública/privada deve ser capaz de impossibilitar a criação de uma chave a partir da outra. Sem essa garantia o método não poderá ser aplicado à autenticação e à certificação, mas somente ao sigilo.

Entre os algoritmos assimétricos, pode-se citar:

a) **Diffie-Hellman** – praticamente o primeiro a ser utilizado para este tipo de criptografia. Foi projetado para permitir a dois indivíduos entrarem em um acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público, não permite ciframento nem assinatura digital;
b) **RSA** – criado por Ron Rivest, Adi Shamir e Len Adlemann em 1977, é o mais utilizado na atualidade. O algoritmo por trás do RSA está na premissa de que é muito fácil multiplicar dois números primos para

obter um terceiro número, porém é muito difícil recuperar os dois primos utilizados na multiplicação a partir daquele terceiro número. Isto é conhecido como fatoração; e

c) **El Gamal** – muito parecido com o RSA, obtém sua segurança da dificuldade de se calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração.

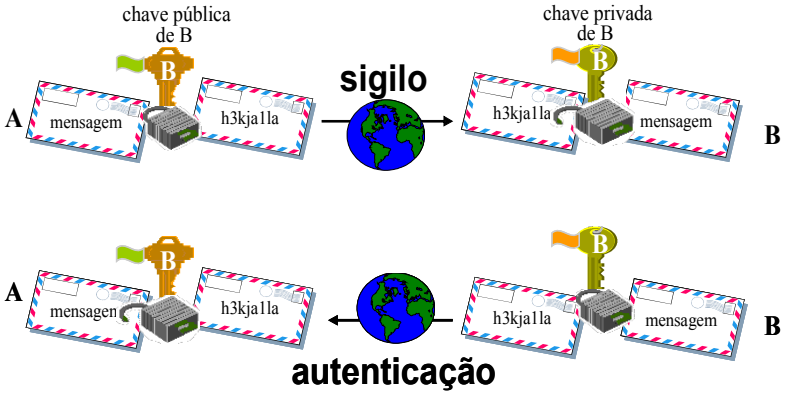


Figura 3: Criptografia assimétrica
Fonte: Autor

2.3.4 FUNÇÃO HASH

Uma função é chamada *hash*, ou dita unidirecional, quando possui a característica de transformar uma entrada de tamanho variável, em um resultado na saída de tamanho fixo. Também vale ressaltar que uma de suas maiores características esta na facilidade de ser calculada e a grande dificuldade em se obter o resultado inverso, ou seja ser invertida.

Por exemplo, 96 *bits*, também chamada resumo, é uma função computacionalmente muito difícil de ser invertida, não sendo possível, a partir do resultado da função *hash*, se chegar ao valor utilizado na sua entrada. Logo, o resultado dessa função corresponderá a um valor de entrada, e se este valor for alterado, o resultado da saída também será diferente, com exceção das colisões, que podem ocorrer devido ao número de possibilidades na entrada ser muito maior do que os números na saída.

No entanto, com o exemplo de uma saída de 96 *bits*, ter-se-á 2 elevado a 96 possibilidades na saída, portanto a probabilidade de ocorrer colisões torna-se tanto quanto desprezível.

Um outro exemplo bastante didático e simples de uma função unidirecional, porém não aplicada à criptografia, é o cálculo do resto da divisão de um número por outro. Se, por exemplo, criar-se uma função que calcule o resto da divisão de qualquer número por 10 o que temos é que qualquer que seja o número que será dividido por 10 o resultado é sempre um número entre 0 e 9. Isto é, o processo de cálculo é bem simples.

Porém, como saber se o resultado do resto for, por exemplo 9. Qual foi o número que, divido por 10, gerou resto 9. É muito difícil afirmar, com certeza, visto que existem infinitos números que divididos por 10 darão resto 9.

A esse fato dá-se o nome de colisão. Isto é, quando dois números diferentes aplicados à função de *hash* geram o mesmo resultado dizemos que houve uma colisão. Nesse ponto é que se faz a diferença entre uma função de *hash* criptográfica e uma não criptográfica. A função *hash* criptográfica é aquela que foi elaborada para possuir o mínimo de colisões possíveis.

Este tipo de função é normalmente usada para efetuar cálculos de integridade de mensagens. Isto ocorre por uma característica muito peculiar da função *hash*. O tamanho do seu resultado é sempre fixo e pequeno. Uma função *hash* tem em média 20 *bytes* de saída, independente do tamanho do texto de entrada.

A função é normalmente utilizada da seguinte forma para cálculo de integridade:

a) obtém-se mensagem *M;*
b) obtém resultado do *hash D,* onde *D* = h(*M*); e
c) envia/Armazena *M* e *D.*

O processo de verificação de integridade é o seguinte:

a) obtém-se *M* e *D;*
b) calcula-se novamente o hash da mensagem *D'* onde *D'* = h(*M*);
c) compara-se *D* com *D'* para ver se são iguais; e
d) se *D* e *D'* são iguais, então a mensagem está íntegra, o contrário não.

Exemplos de Algoritmos Hash:

a) **MD5** – A sigla MD significa *Message Digest*. Este algoritmo foi desenvolvido por Ron Rivest para operação de resumo de mensagens e produz um valor *hash* de 128 *bits;* e
b) **SHA-1** – *Secure Hash Algorithm* é uma família de algoritmos para operação de resumo de mensagens criado pela Agência de Segurança Nacional (NSA) *National Security Agency* para ser o sucessor do MD5. O SHA-1 gera um valor *hash* de 160 *bits*, a partir de um tamanho arbitrário de mensagem.

Figura 4: Integridade com a função *hash.*
Fonte: Autor.

2.4 MECANISMOS DE ASSINATURA DIGITAL

Quando se começou a falar de assinatura digital era muito comum se ouvir comentários que a simples digitalização de uma imagem da assinatura manuscrita era suficiente para alcançar esse propósito, porém esta hipótese se tornava extremamente simplória quando se imaginava que a assinatura digitalizada poderia ser copiada e anexada a qualquer outro tipo de documento tornando-a simples de ser forjada.

Criados com o objetivo de substituir a assinatura manuscrita por uma que proporciona-se as mesmas garantias do mundo real por meio da TI, a assinatura digital surgiu com base em analogia ao processo convencional, onde um sinal gráfico (pessoal) é posto em um papel para ratificar seu conteúdo. O processo torna-

se válido porque este sinal gráfico fica atrelado ao papel, supostamente de forma permanente.

Vale lembrar que este processo tradicional não é completamente seguro, uma vez que é possível por meio de vários artifícios apagar, copiar de forma idêntica, transcrever ou até mesmo modificar uma assinatura por uma pessoa habilidosa.

O processo de assinatura digital se utiliza de algoritmos criptográficos assimétricos criados com base na teoria da entropia visando o embaralhamento de um número pequeno oriundo de uma função chamada *hash*, que posteriormente será anexada ao arquivo que se deseja transmitir. O resultado desse processo é chamado de assinatura digital.

O processo de verificação utiliza a chave par assimétrica para comparação do número *hash* gerado anteriormente com o novo número gerado no momento que o referido arquivo será lido.

Note que as características descritas da assinatura digital possuem princípios idênticos à assinatura tradicional que se conhece (assinatura pessoal privada x constatação e verificação pública).

Na assinatura digital o reconhecimento da firma sempre envolve o conteúdo da mensagem, pois a comparação é feita sobre o *hash* da mensagem e não sobre o texto da mesma. Qualquer adulteração do texto original torna a verificação da assinatura incorreta, uma vez que calculado o *hash* de uma mensagem o processo não pode ser revertido. Dessa forma, a única maneira de se comparar mensagens é fazendo a comparação do *hash* das mesmas.

2.5 ASSINATURA DIGITAL

Este serviço é análogo à assinatura do próprio punho, que estabelecendo os mesmos princípios filosóficos e conceituais da assinatura tradicional, trouxe para o mundo digital a possibilidade de se assinar uma mensagem, e esta ser lida por qualquer outro ator e verificar sua autenticidade.

Este serviço eletrônico utiliza-se da criptografia assimétrica para ser realizado, com uma chave pública e outra privada e é executado o processo

utilizando-se uma função *hash* para criar um número chamado de resumo da mensagem a qual se quer assinar (*Message Digest*), que é em seguida cifrada com a chave privada do ator que a está assinando.

Em seguida, para se obter a verificação da assinatura, o receptor, utilizando a chave pública do assinante, descriptografa o resumo da mensagem e executa a função *hash* sobre a mensagem visando obter um outro resumo que é comparado com o primeiro.

Entre os algoritmos mais utilizados para a criptografia do resumo (*hash*) obtido sobre uma mensagem temos o RSA, El Gamal e DSA.

A segurança está em que somente o autor pode criptografar o resumo daquela mensagem oriunda da função *hash*, pois somente ele possui a sua senha pessoal que também poderá ser descriptografada pelo outro par de sua chave, chamada de chave pública.

Para utilização desse método, cada ator deve possuir um dos pares de chaves assimétricas e deve, também, haver um mecanismo para distribuição das chaves, neste caso a rede WAN ou Internet ou ainda uma intranet, bem como a certificação de uma associação que garanta a transação realizada.

O processo é muito simples e pode ser aplicado não somente a um texto, mas também a qualquer tipo de arquivo digital (imagem, som, etc).

Assim um processo de assinatura digital poderia ser resumido da seguinte forma:

Assinatura:

a) obtém-se a mensagem M e a chave privada (d, n) do assinante;
b) extrai-se o número hash da mensagem M;
c) realiza-se a criptografia do número hash com a chave privada;
d) obtém-se a assinatura da mensagem $A = h(M)^d \bmod n$; e
e) envia-se a mensagem M e a assinatura A.

Figura 5: Assinatura digital com chaves públicas.
Fonte: https://www.oficioeletronico.com.br/Downloads/CartilhaCertificacaoDigital.pdf.

Reconhecimento da Assinatura:

a) obtém-se a mensagem M, a assinatura A e a chave pública (e, n);
b) obtém-se o hash da mensagem h(M') decriptando-se A com a chave pública $h(M') = A^e \bmod n$; e
c) compara-se o *hash* da mensagem original h(M) com a mensagem decriptada h(M'). Se os dois hashs são iguais, então a assinatura está correta.

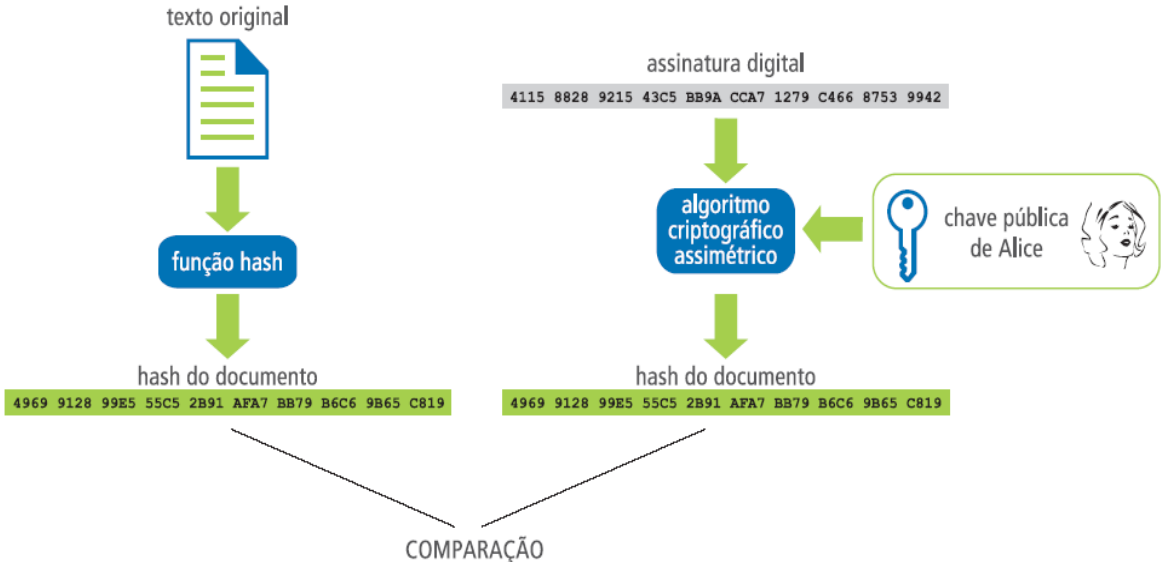


Figura 6: Conferência da assinatura digital.
Fonte: https://www.oficioeletronico.com.br/Downloads/CartilhaCertificacaoDigital.pdf.

2.6 CERTIFICADO DIGITAL

Um certificado digital pode ser definido como um documento eletrônico, assinado digitalmente por uma terceira parte confiável, que associa o nome (e atributos) de uma pessoa ou instituição a uma chave criptográfica pública.

Em um grupo pequeno, é possível cada ator trocar, pessoalmente, sua chave pública com o outro, e assim todos do grupo estarão habilitados a verificar a assinatura um do outro. Porém, em uma grande rede, essa situação torna-se impossível, uma vez que, torna-se inviável reter em um computador a chave pública de milhares de atores dispersos por todo mundo

Uma solução encontrada para este problema foi trabalhar com delegação de confiança. Uma pessoa passa a aceitar a chave pública de outra desconhecida, simplesmente por existir um terceiro ator no processo a qual ela conhece e confia.

Na verdade, o que acontece nesse processo é o mesmo que aconteceria se uma pessoa levasse um documento no cartório para que se realizasse o reconhecimento de firma daquele que assinou um documento, a pessoa aceita a assinatura como verdadeira porque confia na instituição que dá a chancela afirmando que aquela assinatura é verdadeira.

No mundo digital entidades confiáveis designadas Autoridades Certificadoras (AC), tais como as empresas Verisign, Cybertrust, Nortel, ou órgãos governamentais como o SERPRO, Receita Federal, Banco do Brasil e Presidência da República, assinam eletronicamente um documento chamado Certificado Digital, contendo os dados de uma pessoa e sua chave pública, garantindo sua validade.

De posse da chave pública da AC, qualquer indivíduo pode verificar a assinatura do certificado digital e ter certeza que a chave pública contida nele pertence à pessoa nominada no mesmo.

Assim, para se verificar a assinatura de alguém basta guardar a chave pública da AC que a emitiu e, sempre que for necessário, checar a autenticidade de uma assinatura. Esse procedimento verifica apenas o certificado do assinante emitido pela AC.

Desta forma, em vez de guardar um grande número de chaves públicas no seu computador, somente é necessário guardar a chave pública da sua AC.

Ou seja, um certificado digital é basicamente um documento eletrônico assinado digitalmente que associa as informações públicas de uma pessoa ou entidade a uma chave pública.

Um Certificado Digital normalmente apresenta as seguintes informações:

a) nome da pessoa ou entidade a ser associada à chave pública;
b) período de validade do certificado;
c) chave pública;
d) nome e assinatura da entidade que assinou o certificado;
e) número de série.

Logo abaixo temos uma figura de um certificado digital da ICP-Brasil retirado de um browser rodando no sistema operacional Windows.

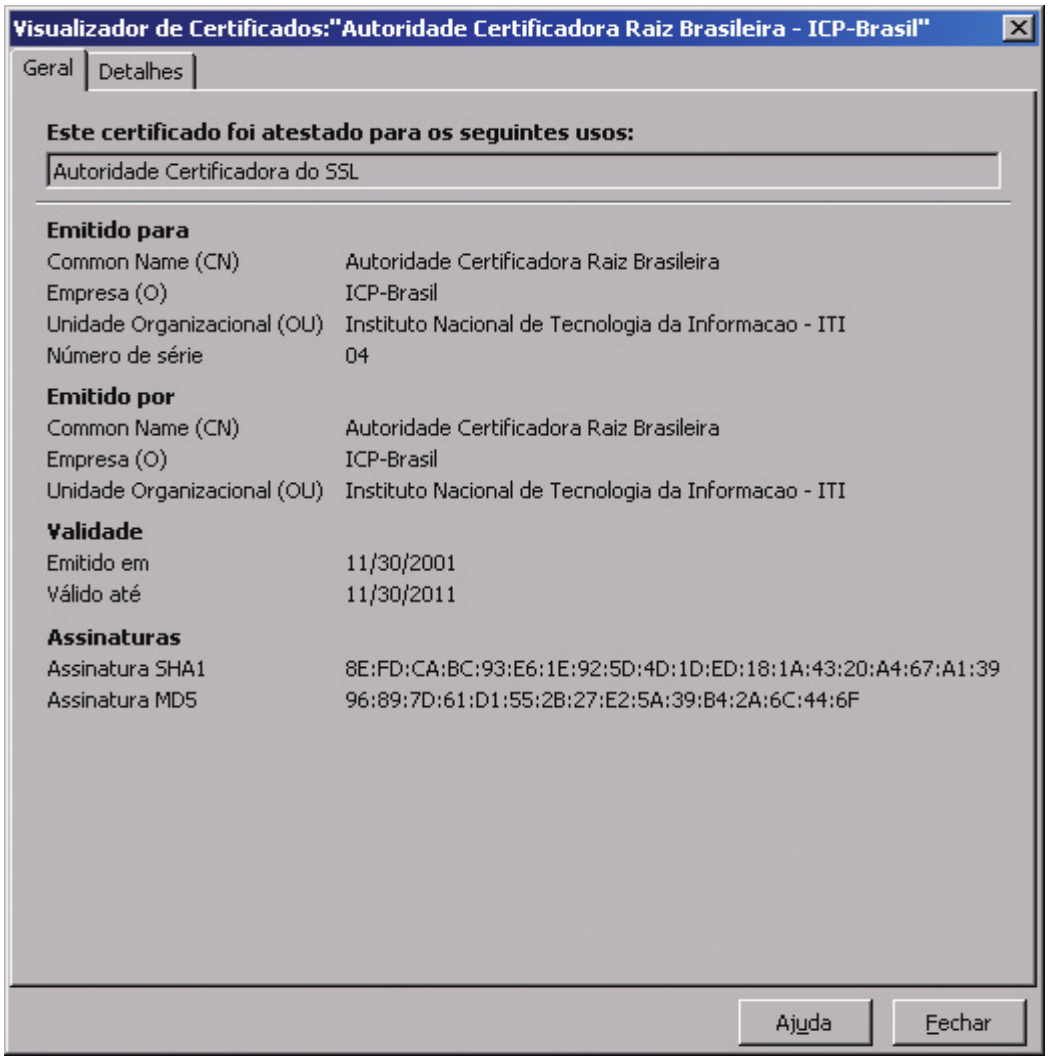


Figura 7:Certificado Digital da Autoridade Certificadora Raiz Brasileira
Fonte: www.iti.gov.br/twiki/pub/Certificacao/.../brochura01.pdf

2.7 SEGURANÇA DA CHAVE PRIVADA

Como foi visto anteriormente, o certificado digital garante a segurança da chave pública de alguém. Porém, só isso não evitaria os problemas oriundos da falta de proteção da chave privada de um ator.

Qualquer pessoa que tenha acesso à chave privada de outro, pode se passar por ele, visto que passa a assinar pela pessoa. Por essa razão, o proprietário da chave privada deve ter muita preocupação em manter o sigilo da sua chave.

Pensando nisso é que foram desenvolvidos vários processos que minimizam a perda da assinatura, evitando o seu uso mal intencionado.

Guardar em um cofre um disquete com a sua chave privada. Esse processo é seguro porém muito burocrático, uma vez que a chave não pode ser levada para outros lugares.

Cifrar a chave com senha que somente o dono conheça. Esse é um processo bom, pois a chave cifrada pode ser guardada em um disquete e levada para qualquer lugar. O inconveniente é que, se a senha for fraca, alguém que tenha acesso a chave cifrada pode efetuar tentativas múltiplas de decifra-lá.

Guardar a chave privada em *smart-cards* (cartões inteligentes). Esse processo resume-se em cartões que possuem um *chip* interno à prova de invasão e somente podem ser acessados através de uma senha ou algum tipo de biometria (impressão digital por exemplo). Esses cartões possuem ainda a possibilidade de fazer pequenos processamentos internos gerando um par de chaves assimétricas que protegem a chave privada contra qualquer tipo de invasão.

Além disso, o *chip* contém mecanismos de autodestruição, caso seja rompido, ele ainda impede tentativas sucessivas de se obter a senha, pois bloqueia automaticamente o funcionamento após um número determinados de tentativas.

Guardar a chave privada em *tokens* (*pen drive* de pequena capacidade) este processo é o mais confiável atualmente, pois, como no *smart-cards,* podem conter pequenos programas capazes de fazerem pequenos processamentos internos gerando par de chaves assimétricas, que protegem a chave privada, além de possibilitar o transporte com extrema facilidade.

Torna-se interessante frisar que os usuário detentores de *tokens* e *smart-cards* jamais possuem acesso ao conteúdo do token ou cartão. Ele somente solicita ao *token* ou cartão que faça determinado tipo de ação, no caso, que efetue uma transação bancária ou assine um documento digital usando a chave privada do proprietário. Essas ações somente são executadas se o possuidor do cartão ou *token* digitar corretamente a senha de acesso ou fornecer a sua impressão digital.

Figura 8: Smart-cards com Certificado Digital da Receita Federal
Fonte:http://www.receita.fazenda.gov.br

Figura 9: Smart-cards e token com Certificado Digital
Fonte: http://www.certisign.com.br/certificacao-digital/por-dentro-da-certificacao-digital

4.6 RESPONSABILIDADE

A certificação digital traz diversas facilidades, porém seu uso não torna as transações realizadas isenta de responsabilidades. Ao mesmo tempo que o uso da chave privada autentica uma transação ou um documento, ela confere o atributo de não-repúdio à operação, ou seja, o usuário não pode negar posteriormente a realização daquela transação. Por isto, é importante que o usuário tenha condições de proteger de forma adequada a sua chave privada.

Existem dispositivos que incrementam a proteção das chaves, como os cartões inteligentes (smart cards). Eles se assemelham – em formato e tamanho – a um cartão de crédito convencional. Os smart cards são um tipo de hardware criptográfico dotado de um microprocessador com memória capaz de armazenar e processar diversos tipos de informações. Com eles é possível gerar as chaves e mantê-las dentro de um ambiente seguro, uma vez que as operações criptográficas podem ser realizadas dentro do próprio dispositivo.

Alguns usuários preferem manter suas chaves privadas no próprio computador. Neste caso, são necessárias algumas medidas preventivas para minimizar a possibilidade de se comprometer a sua chave privada:

a) caso o software de geração do par de chaves ofereça a opção de proteção do acesso à chave privada através de senha, essa opção deve ser ativada, pois assim há a garantia de que, na ocorrência do furto da chave privada, a mesma esteja cifrada;
b) não compartilhar com ninguém a senha de acesso à chave privada;
c) não utilizar como senha dados pessoais, palavras que existam em dicionários ou somente números, pois são senhas facilmente descobertas. Procurar uma senha longa, com caracteres mistos, maiúsculos e minúsculos, números e pontuação;
d) em ambiente acessível a várias pessoas, como em um escritório, usar produtos de controle de acesso ou recursos de proteção ao sistema operacional, como uma senha de sistema ou protetor de tela protegido por senha;
e) manter atualizado o sistema operacional e os aplicativos, pois versões

mais recentes contêm correções que levam em consideração as vulnerabilidades mais atuais;

f) não instalar o certificado com a chave privada em computadores de uso público.

Em caso de suspeita de comprometimento da chave privada, seja por uma invasão sofrida no computador ou pelo surgimento de operações associadas ao uso da chave que não sejam de conhecimento do seu proprietário, a revogação do certificado deve ser solicitada o mais rapidamente possível à AC responsável pela sua emissão. Além disso, é necessário estar alerta às recomendações da DPC quanto aos procedimentos

Neste capitulo foi possível entender os mecanismos da assinatura digital o significado do certificado digital, sua utilidade e a necessidade da existência de uma AC ratificando e garantindo as transações. Agora torna-se fácil entender a importância da AC responsável por identificar os agentes, receber a chave pública e emitir um certificado para ela, mas essas atividades inerentes a AC veremos logo a frente no capitulo que trata das atribuições das AC.

2.9 ALGORITMOS UTILIZADOS PELA ICP – BRASIL

Viu-se que a assinatura digital é gerada a partir da conjugação de dois algoritmos criptográficos: o algoritmo de criptografia assimétrico, cuja principal característica é a presença de um par de chaves; e o algoritmo criptográfico de função hash, cuja principal característica consiste no seu processo unidirecional.

Do arquivo que deverá ser assinado, calcula-se o resumo criptográfico, por meio da utilização de um algoritmo de função hash. Sobre o resumo hash aplica-se a criptografia assimétrica, utilizando a chave privada.

Desta forma observa-se que a assinatura depende de dois algoritmos criptográficos com características diferentes. Um que realiza a criptografia assimétrica, composto por um par de chaves, responsável pela geração da assinatura; e outro denominado de função hash, que reduz o arquivo em um pequeno bloco alfanumérico de informações irreversíveis.

Em linhas gerais, a escolha do algoritmo de criptografia assimétrico e do algoritmo criptográfico de função hash é muito importante, pois estão intrinsecamente relacionados à integridade do documento.

A ICP-Brasil, com o objetivo de assegurar a integridade dos documentos eletrônicos assinados digitalmente aponta, por meio de atos normativos, quais os algoritmos que deverão ser usados. Consoante disserta a Declaração de Práticas de Certificação da AC-Raiz (Resolução n.o 1, do C.G.), em seu item 7.1.3, o certificado digital da AC-Raiz é assinado com um algoritmo criptográfico assimétrico RSA, utilizando-se do SHA-1 como algoritmo criptográfico de função de hash.

Nesta linha, a resolução n.o 7, de 12 de Dezembro de 2001, do C.G., aprovando os requisitos mínimos para políticas de certificado, no item 7.1.3 determina que serão admitidos no âmbito da ICP-Brasil, como algoritmos criptográficos utilizados para assinar os certificados emitidos ao usuário final os seguintes: RSA122; SHA-1123 com RSA; MD5124 com RSA; e SHA-1 com DSA125.

Todavia, em 18 de maio de 2006, através do DOC ICP-01.01 – V 1.0, do Instituto Nacional de Tecnologia da Informação, ficou estabelecido que os algoritmos criptográficos que deverão ser utilizados para a assinatura de certificados de AC deverão ser necessariamente o SHA-1 com RSA, e os algoritmos criptográficos que deverão ser utilizados para assinar certificados dos usuários deverão ser o SHA 1 com RSA ou o SHA 1 com DSA.

O RSA vem descrito na RFC 2313. Os RFC constituem uma categoria de documentos que descreve padrões da Internet. É proveniente do IETF (*Internet Engineering Task Force*) que é uma comunidade internacional composta por membros de vários setores interessados, preocupados com a evolução da arquitetura da Internet e seu perfeito funcionamento.

- O SHA-1 vem descrito no FIPS 180-1. É um documento de Publicação Federal de Padrões de Processamento de Informações emitido pelo NIST (*National Institute of Standards and Technology*).

- O MD5 vem descrito na RFC 1321.

- O DSA é um algoritmo criptográfico assimétrico, assim como o RSA, usado apenas para gerar a assinatura digital sobre o resumo da função de hash, não servindo para ser usado como criptografia de dados.

2.10 ALGORITMO DE FUNÇÃO HASH MD5

O MD5, corresponde à abreviatura da expressão "*Message-Digest Algorithm 5*, consistindo num algoritmo de hash, com tamanho de 128 bits. Criado em 1992, por Ron Rivest, através da empresa RSA, localizada em Bedford, em Massachusetts, nos Estados Unidos, utilizado largamente como ferramenta para assegurar integridade de informações em formato eletrônico.

Todavia, em 1993 (Xiaoyan, 2004)126 , Bert den Boer e Antoon Bosselaus encontraram pseudo colisões no MD5, consistindo numa mesma mensagem com 02 diferentes grupos de valores iniciais. De acordo com a pesquisa, os ataques demonstraram uma grande fragilidade no bit do MD5 mais significativo.

Foi permitida a utilização do MD5, como função de hash, pelos órgãos públicos brasileiros desde a criação da atual ICP-Brasil, conforme podemos verificar pela Resolução no 7 do Comitê Gestor da ICP-Brasil127.

Em linhas gerais, conforme explica Xiaoyan (2004)128, o algoritmo MD5 é compreendido pela função matemática de x = f(z). Podemos compreender que "z" representa os bits existentes em uma mensagem, e "x" representa o valor de hash obtido através do algoritmo de hash.

Esse ataque, denominado de "ataque diferencial modular" tem como base um bloco codificado, no qual através de uma função XOR (ou exclusivo) parte-se de dois blocos diferentes de informação, obtendo-se o mesmo resumo criptográfico. Para a realização desses testes, foi utilizado um supercomputador IBM P690, e os testes duraram algumas horas até a obtenção dos primeiros resultados.

Klima (2005)129, propondo um método aperfeiçoado a partir daquele construído pela equipe chinesa, conseguiu melhores resultados, utilizando-se daquilo que se denominou de inicialização de vetores. Consoante bem descreve o autor, a contribuição de sua pesquisa está na diminuição do tempo utilizado para o encontro de colisões, ocorrendo em no máximo 2 minutos, utilizando-se um simples

notebook de 1.6 Ghz, enquanto que a equipe chinesa levou algumas horas para conseguir os mesmos resultados, com a utilização de um supercomputador.

Vale ressaltar que o ganho de tempo com o método proposto por Klima somente é atingido na primeira colisão, sendo que numa segunda colisão, o método proposto pela equipe chinesa demonstrou-se mais eficiente.

Nesta linha, a equipe chinesa demonstrou dois pares de colisão de mensagens, enquanto que no trabalho de Klima (2005)130 foram apresentados 04 pares de colisão de mensagem, suficiente para a realização de ataques bem sucedidos de falsificação contra documentos eletrônicos.

A fragilidade do MD5 fica ainda mais evidente quando analisamos os trabalhos de Kim (2005)131 e Stevens (2006)132.

No primeiro trabalho, foram exploradas propostas em "*related-key rectangle and boomerang*" utilizando técnicas não randômicas de MD5 distinguindo-o de uma cifra aleatória escolhida.

No segundo trabalho, Stevens apresenta um aperfeiçoamento dos ataques ao algoritmo hash MD5 para encontrar dois blocos de colisão, utilizando-se das mesmas condições e caminhos propostos pelo grupo de pesquisa chinês. A nova técnica baseia-se no cumprimento de determinadas limitações, possibilitando a mudança dos diferenciais do primeiro ciclo. Para o segundo ciclo, Stevens utiliza o método empregado alhures por Klima.

Por conseguinte destaca Klima (2005)134 a comunidade científica para que se ficasse bastante atento ao usar o MD5 como função hash, uma vez que ele não mais conseguia assegurar seu principal propósito, a integridade dos dados.

2.11 ALGORITMO DE FUNÇÃO HASH SHA-1

O *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia) – NIST – é um organismo do governo norte americano com responsabilidade de emitir padrões criptográficos na realização de assinaturas digitais.

Em primeiro de agosto de 2002, o NIST editou o documento Federal *Information Processing Standards Publication* (Publicação Federal dos Padrões de

Processamento de Informações) sob o n.o 180-2. Neste documento restou acordado que o algoritmo de hash SHA-1 é suficientemente seguro para condensar representações computacionais eletrônicas, ou seja, é seguro para ser utilizado na realização de assinaturas digitais.

O SHA-1 (Secure Hash Algorithm) foi criado pelo NIST em 1994, como um avanço do SHA-0, sendo hoje considerado um algoritmo de hash confiável dado que a realização de ataques é computacionalmente inviável.

São características de código hash viável:

a) resistência a primeira inversão, onde dado o bloco de hash é computacionalmente improvável a obtenção da mensagem original;
b) resistência à segunda inversão, sendo computacionalmente improvável que se encontre uma outra mensagem que se utilizando de mesma função hash encontre o mesmo bloco; e
c) resistência a colisões, sendo improvável que duas mensagens distintas gerem o mesmo resumo.

O SHA-1 utiliza uma sequencia de funções lógicas f0, f1.....f79.

Cada função ft, onde 0 <= t < 79, opera em três códigos “x”, “y” e “z”, gerando código de saída de 32 bits de constante 280. Em linhas gerais, temos como entrada um arquivo qualquer em formato digital com um tamanho de até 280 bits, obtendo na saída um resumo criptográfico de 160 bits.

Atualmente segundo o documento ICP-01.01–2006 (Padrões e Algoritmos Criptográficos da ICP-Brasil), o algoritmo criptográfico adotado pela ICP-Brasil para a realização das assinaturas digitais é o SHA-1, todavia a segurança deste algoritmo está sendo abalada. A mesma equipe chinesa liderada por Xiaoyun (2005), responsável pela primeira quebra do MD5, desenvolveu novas técnicas capazes de encontrar colisões na função de hash SHA-1.

A base do ataque aplicado ao SHA-1 é encontrada no ataque diferencial original aplicado ao SHA-0, assim como na busca de colisão do MD5.

Sua resistência foi reduzida de 280 para 263. Com isso conseguiram reduzir o tempo de quebra do SHA-1 pela força bruta em 2000 vezes.

Entretanto, esta redução não representa atualmente um perigo em potencial, a ponto de ser afastado o uso do SHA-1, mas demonstra que o SHA-1 é vulnerável, tendo seu tempo de vida útil reduzido.

Assim como para o MD5, a vulnerabilidade do SHA-1 foi possível por meio da utilização de um supercomputador. Vale ressaltar que na primeira quebra do MD5, pela equipe chinesa, também foi utilizado um supercomputador, e com base nessas pesquisas iniciais, outros pesquisadores conseguiram reduzir o tempo de quebra do MD5 em prazos desconsiderados, como 2 minutos, utilizando-se de um simples notebook de 1.6 Ghz. Quanto tempo mais o SHA-1 conseguirá resistir aos ataques?

O NIST prevê que o SHA-1 será definitivamente abandonado em 2.012, conforme prevê a FIPS 180-2 do NIST. Com isso, a tecnologia deverá se preocupar em continuar a conferir força valorativa aos documentos eletrônicos assinados digitalmente com o SHA-1 como técnica de função hash.

2.12 ESTRUTURA REGULADORA DA CERTIFICAÇÃO DIGITAL

A certificação digital não é um tema novo. Pode-se observar que tal assunto é tratado por vários países desde o início dos anos 90. Antes de se apresentar os modelos iniciais de certificação digital, será feita uma imersão no modelo brasileiro e que, ao ser entendido, fornecerá as informações necessárias para uma comparação com o que ocorre no mundo.

No Brasil, o primeiro esforço regulador ocorreu no ano de 2000. No ano seguinte, em 2001 foi criada, legalmente, a infraestrutura de chaves públicas brasileiras a ICP – Brasil. A ICP Brasil trata-se basicamente de uma estrutura formal, composta por entidades e por um conjunto de normas e leis, que dão sustentação a certificação digital no país e, por conseguinte, ao uso da assinatura digital.

A lei nº 9983, de 2000, alterou o decreto nº 2848, de 1940, do código penal brasileiro, definindo a questão dos crimes digitais, e a medida provisória nº 2200-2 de 24 de agosto de 2001, instituiu a infraestrutura de chaves públicas brasileiras (ICP-Brasil), transformando o ITI (Instituto Nacional de Tecnologia da Informação) em autarquia e apresentou o modelo inicial normativo, bem como

instituiu o comitê gestor da ICP Brasil. A partir desse ato político, começou legalmente o trabalho de estruturação do que hoje vem a ser essa atividade.

2.13 MODELO BRASILEIRO

Segundo Lino Sarlo da Silva, em seu livro, "*Public Key Infrastructure PKI*", o modelo brasileiro de PKI (*Public Key Infrastructure*) possui basicamente três atores fundamentais:

a) **ITI** - (O Instituto Nacional de Tecnologia da Informação): é uma autarquia Federal vinculada à Casa Civil da Presidência da República, responsável pelas ações operacionais da ICP, onde basicamente encontramos as instalações e a operação da sala cofre da Autoridade Certificadora Raiz (AC Raiz), que detêm as chaves públicas de certificação digital, além de ser responsável por emitir, expedir, distribuir, revogar e gerenciar os certificados das Autoridades Certificadoras (AC) de nível imediatamente subsequente ao seu. Compete ainda ao ITI estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico, voltados à ampliação da cidadania digital. Neste vetor, o ITI tem como sua principal linha de ação a popularização da certificação digital e a inclusão digital, atuando sobre questões como sistemas criptográficos, software livre, hardware compatíveis com padrões abertos e universais e a convergência digital de mídias;

b) **comitê gestor da ICP**: composto por membros da sociedade civil e do estado, tendo como função primordial a discussão, que a aprovação do conjunto de normas e ações que regularão as operações da ICP-Brasil e do ITI; e

c) **ICP-Brasil**: É um conjunto de técnicas, práticas e procedimentos, a ser **implementado** pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública.

Na figura seguir pode-se observar como esta estrutura está montada.

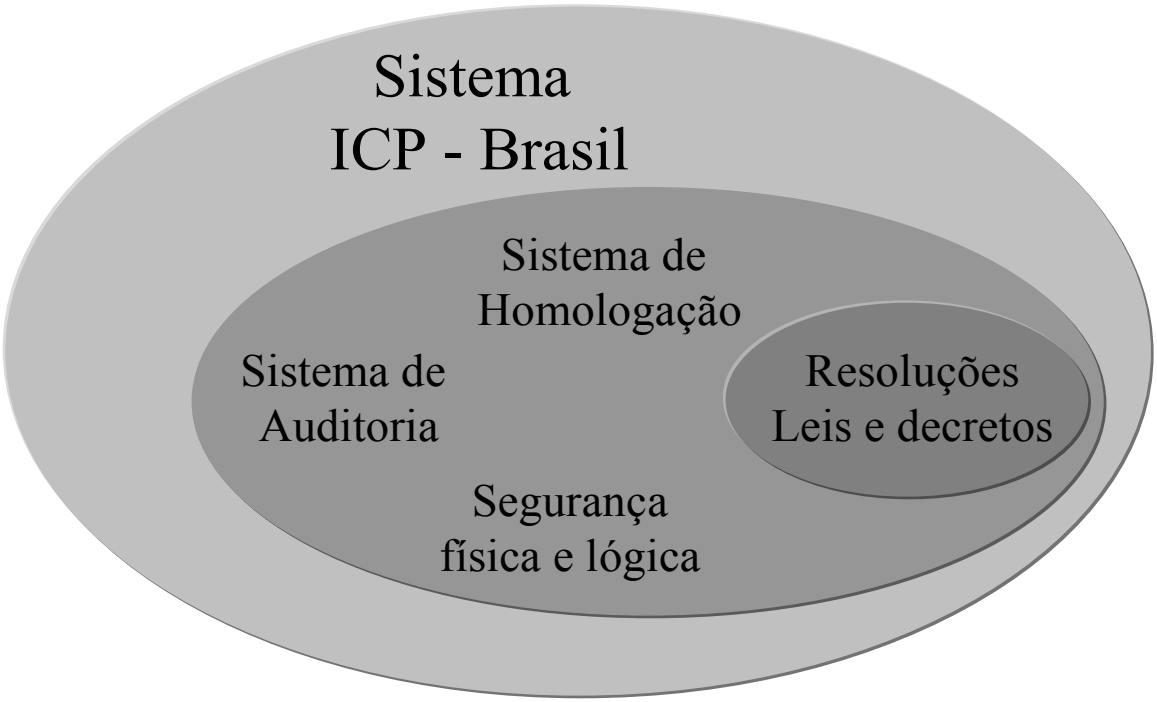


Figura 10: Modelo Brasileiro.
Fonte: Autor.

2.14 RESOLUÇÕES, LEIS E DECRETOS

A ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira - foi instituída pela Medida Provisória 2.200 e, em julho de 2001, as atividades do Comitê Gestor ICP-Brasil foram regulamentadas e redefinidas pelo decreto 3.872.

Basicamente as Leis e os decretos são de inteira responsabilidade do poder Executivo e do Legislativo, porém, as resoluções que regem o modelo operacional, ou seja o núcleo da ICP, são produzidas pelo comitê gestor.

2.15 SISTEMA DE HOMOLOGAÇÃO

Qualquer produto, seja hardware ou software, que venha a compor alguns dos processos de certificação, devem necessariamente passar por um processo de homologação, visando garantir a interoperabilidade e a própria integridade das ações por ele executadas. Hoje existem laboratórios credenciados que executam esse trabalho e, após a aprovação do produto, eles recebem um selo da "*ICP*

compliance". A definição pela necessidade de acomodação de produtos segue uma tendência mundial, que visa dar maior robustez ao modelo, pois sabemos que os fabricantes muitas vezes são ávidos pelo lançamento de novos serviços e produtos, o que no limite, poderia causar uma janela de fragilidade ou mesmo uma incompatibilidade de padrões. A homologação é uma garantia a mais dentro de um modelo que preza pela confiabilidade e segurança.

2.16 SISTEMA DE SEGURANÇA FÍSICA E LÓGICA

Trata-se basicamente de ambientes seguros, onde são depositados os equipamentos e sistemas das Autoridades Certificadoras. Nesses ambientes temos também a geração de certificados revogados, bem como a geração das chaves públicas, que compõe o par de chaves da certificação. Está reservado um capítulo para uma descrição mais detalhada da operação de assinatura digital, por se tratar de um sistema que preza pela segurança e a inviolabilidade dos dados. Esses ambientes são redundantes, ou seja: existe o que chamamos de *"site backup".*

2.17 SISTEMA DE AUDITORIA E FISCALIZAÇÃO

Trata-se da fiscalização, em campo, das normas emitidas pela ICP e suas aplicabilidades. As AC's que não estiverem de acordo com os padrões de processos e operações mínimos, definidos anteriormente, perderão a autorização de funcionamento. Essa atividade, como dito anteriormente, é executada pelo ITI.

2.18 ICP BRASIL

ICP, ou Infraestrutura de Chaves Públicas, é a sigla no Brasil para PKI - *Public Key Infrastructure*, um conjunto de técnicas, práticas e procedimentos a ser implementado pelas organizações governamentais e privadas brasileiras, com o objetivo de estabelecer os fundamentos técnicos e metodológicos elaborados para suportar um sistema criptográfico com base em certificados digitais.

A ICP Brasil apresenta duas estruturas, uma operativa e a outra normativa. a estrutura normativa é formada pelo comitê gestor e por uma comissão de assessoramento técnico (COTEC). Dentro da estrutura cooperativa, que tem na sua raiz o ITI, encontra-se a cadeia de certificação, que será melhor visualizado no item seguinte(Árvore de Certificação). As entidades que suportam as ações descritas anteriormente podem ser apresentadas de acordo com a estrutura exposta na figura a seguir:

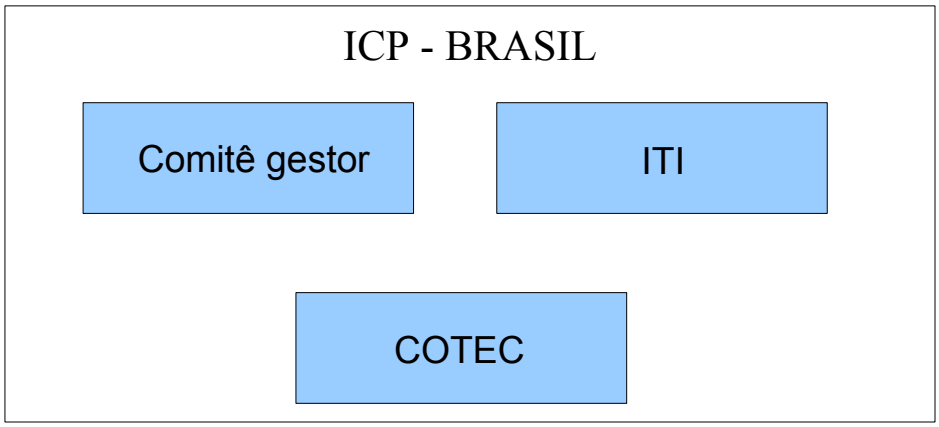


Figura 11: Estrutura da ICP – Brasil.
Fonte: Autor.

2.19 ÁRVORE DE CERTIFICAÇÃO

A estrutura de certificação da ICP-Brasil se desenvolve em forma de uma árvore de certificação. Na base encontramos a Autoridade Certificadora Raiz, que possui como atividade principal a geração de chaves públicas para as AC's primeiro nível, bem como a geração da lista dos certificados revogados dessas AC's.

Na ICP-Brasil, a função de AC Raiz é exercida pelo ITI, uma autarquia pública a ligada à Presidência da República.

Seguindo a árvore de certificação, observamos a existência das AC's de primeiro e segundo nível. As primeiras são aquelas que são inicialmente credenciadas pelo ITI para a execução da certificação. As AC's que delas surgem, são conhecidas como AC's subsequentes e tem toda a solidariedade operacional e legal da AC de primeiro nível.

Observando ainda a árvore, encontramos a figura das AR's (autoridades de registro) que executam as funções cartoriais da certificação. São as responsáveis pelo atendimento ao público interessado na aquisição do certificado digital. É na AR que é gerado certificado digital ao cidadão, perante a a apresentação de uma série de documentos.

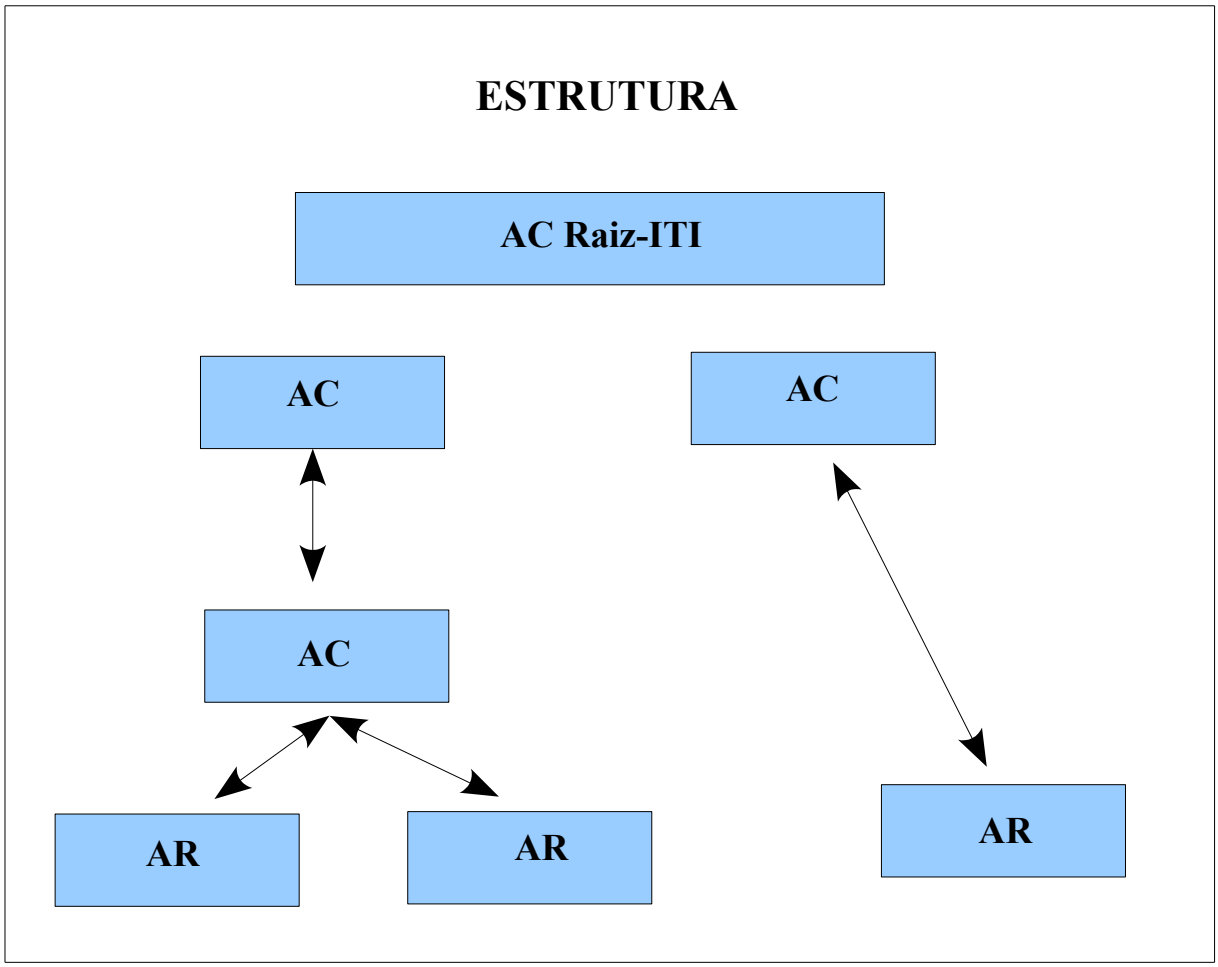


Figura 12: Árvore de certificação.
Fonte: Autor.

2.20 OBRIGAÇÕES DA AC RAIZ

Para o inicio da atividade, comercial ou não, de certificação os atores interessados devem se sujeitar às regras de credenciamento imposta pela IP-Brasil. O cumprimento dos pré-requisitos, definidos em resoluções, é condição necessária para a homologação do credenciamento bem como para o exercício continuado da

atividade de certificação.

As AC's e AR's coligadas, devem ter claramente definidas suas regras de negócio, que se traduzem na forma de sua PC (Políticas de Certificação) e DPC (Declaração de Práticas de Certificação). Essas politicas devem estar consonantes com o que preconiza a ICP. Basicamente essas regras de negócio envolvem acordos de nível de serviços que devem ser cumpridos entre as AC's e os seus clientes bem como entre elas e a ICP-Brasil.

Após cumpridos os requisitos mínimos para o credenciamento destas entidades, por meio de vistoria e homologação por parte do ITI, recebem uma concessão para exercerem suas atividades em seus devidos níveis. Porém o descumprimento de alguma exigência acordada com o ITI faculta ao órgão fiscalizador a solicitação da concessão de funcionamento descredenciando a AC ou AR.

Devido a arquitetura funcional desta estrutura ser baseada na confiabilidade os aspectos de segurança possuem extrema relevância com exigências bastantes rígidas como pode-se observar:

a) emissão e gerenciamento do par de chaves criptográficas;
b) emissão e distribuição do certificado da AC-Raiz;
c) emissão, expedição e distribuição de certificados de AC de nível imediatamente subsequente ao seu;
d) publicação dos certificados por ele emitidos;
e) revogação de certificados por ele emitidos;
f) emissão, gerenciamento e a publicação de sua lista de Certificados;
g) fiscalização e a auditoria das AC, das AR e dos Prestadores de Serviços de Suporte – PSS habilitados em conformidade com o critérios estabelecidos pelo Comitê Gestor da ICP-Brasil;
h) implementação de acordos de certificação cruzada, conforme as diretrizes estabelecidas pelo CG da ICP-Brasil;
i) adotar medidas de segurança e controle, previstas nesta DPC e na Política de segurança da ICP-Brasil, envolvendo seus processos, procedimentos e atividades;
j) manter os processos, procedimentos e atividades em conformidade

com a legislação vigente e com as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;

k) manter e garantir a integridade, o sigilo e a segurança da informação por ele tratada; e
l) manter e testar regularmente seu plano de conformidade de Negócio.

Essa rigidez aplicável à AC raiz, produz contrapartida nas AC que compõem a cadeia de certificação como podemos observar a seguir as obrigações que se estabelecem para as AC de uma forma normativa.

2.21 OBRIGAÇÕES DAS AC

a) operar de acordo com a sua DPC e com as PC que implementa;
b) gerar e gerenciar seus pares de chaves criptográficas;
c) assegurar a proteção de suas chaves privadas;
d) notificar a AC de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do certificado;
e) notificar os seus usuários quando ocorrer suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
f) distribuir o seu próprio certificado;
g) emitir, expedir e distribuir os certificados de AC de nível imediatamente subsequente ao seu ou os certificados de AR a ela vinculadas e de usuários finais;
h) informar a emissão do certificado ao respectivo solicitante;
i) revogar os certificados por ela emitidos;
j) emitir, gerenciar e publicar suas LCR e, quando aplicável, disponibilizar consulta *on-line* de situação do certificado.
k) publicar em sua página web sua declaração de prática de certificação (DPC) e as políticas de certificação (PC) aprovadas que implementa;

l) publicar em páginas *WEB,* informações sobre o descredenciamento da PSS e AR,bem como sobre eventual extinção de instalação técnica;
m) utilizar VPN (*Virtual Private Network*) e SSL (*Secure Socket Layer*) ou outra tecnologia de igual ou superior nível de segurança e privacidade, ao disponibilizar serviços para usuários ou solicitantes de certificados via WEB;
n) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
o) adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP – Brasil;
p) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP – Brasil e com a legislação vigente;
q) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
r) manter e testar anualmente seu Plano de Continuidade do Negócio;
s) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas AC de nível subseqüente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo coma s normas do Comitê Gestor da ICP-Brasil;
t) informar às terceiras partes e titulares de certificado acerca das garantias,coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;
u) informar ao ITI, mensalmente, a quantidade de certificados digitais emitidos;
v) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

A observação das normas de segurança que se estabelecem para as AC nos levam a imaginar que isso trará impactos para as AR, e não poderia ser diferente, várias são as obrigações de segurança para as AR, que por tratarem diretamente com o cliente e executarem a ação cartorial de certificação, trazem consigo algumas especificações, que podem ser observadas a seguir:

2.22 OBRIGAÇÕES DAS AR

a) receber solicitações de emissão ou revogação de certificados;
b) confirmar a identificação do solicitante e a validade da solicitação;
c) encaminhar a solicitação de emissão ou de revogação de cerificado à AC responsável utilizando VPN (*Virtual Private Network* – rede privativa virtual), SSL *(Secure Socket Layer* – protocolo de comunicação seguro*)* ou outra tecnologia de igual ou superior nível de segurança e privacidade;
d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
e) disponibilizar os certificados emitidos pala AC aos seus respectivos solicitantes;
f) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
g) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada;
h) manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecimento nas normas, critérios, práticas e procedimentos da ICP-Brasil;
i) manter e testar anualmente o Plano de Comunidade de Negócios;
j) checar documentos e assinaturas apresentadas;
k) garantir que toda a operação de solicitação de certificados seja realizada em instalações técnicas autorizadas a funcionar como AR.

Dentro ainda da linha de confiabilidade e segurança, não poderia faltar a obrigações que se referem ao usuário dos certificados,que podem vir a se constituir como um elo frágil nessa cadeia.

2.23 OBRIGAÇÕES DO TITULAR DO CERTIFICADO

a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
d) conhecer os seus direitos e obrigações, contemplados pala DPC e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil; e
e) informar à AC emitente qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

Pode-se observar que, cada elemento que compõem a cadeia de certificação possui um leque de obrigações que visa imputar responsabilidades a estes, de maneira a fortalecer e solidificar a cadeia certificadora do ponto de vista da segurança e confiabilidade. Cabe frisar que outros aspectos de segurança são tratados pelas normativas. Como sugestão àqueles que gostariam de se aprofundar nesse aspecto, que busquem consultar as relações da ICP-Brasil.

3 INFRAESTRUTURA DE CHAVES PÚBLICAS DO COMAER

A ICP COMAER é um conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações militares 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, bem como a realização de transações eletrônicas seguras

Sua estrutura, oriunda da Medida Provisória 2.200-2, é formada por um a Autoridade Certificadora Raiz (AC Raiz), Autoridade Certificadora do Comando da Aeronáutica (AC-COMAER), e suas Autoridades de Registros (AR)

3.1 AUTORIDADE CERTIFICADORA DO COMANDO DA AERONÁUTICA

É a entidade integrante da ICP-Brasil em nível imediatamente subsequente à AC Raiz, responsável pela assinatura dos certificados das Autoridades de registro, que por conseguinte é a entidade integrante da ICP-COMAER em nível imediatamente subsequente ao da AC-COMAER, responsável pela emissão e administração dos Certificados Digitais.

O Comando da Aeronáutica estabeleceu em documento orientador de sua estrutura, o qual encontra-se em fase final de elaboração a definição de suas autoridades de registro como as entidades operacionalmente vinculadas à Autoridade Certificadora do Comando da Aeronáutica, responsáveis pela confirmação da identidade dos solicitantes dos certificados credenciamento e habilitação dos usuários finais.

O Comando da Aeronáutica adotou como autoridade de registro (AR) as Seções de Identificação dos Comandos Aéreos Regionais. No caso serão sete autoridades de registro distribuídas pelo território Nacional, cada uma responsável por uma área de jurisdição que somadas corresponderão ao território Brasileiro.

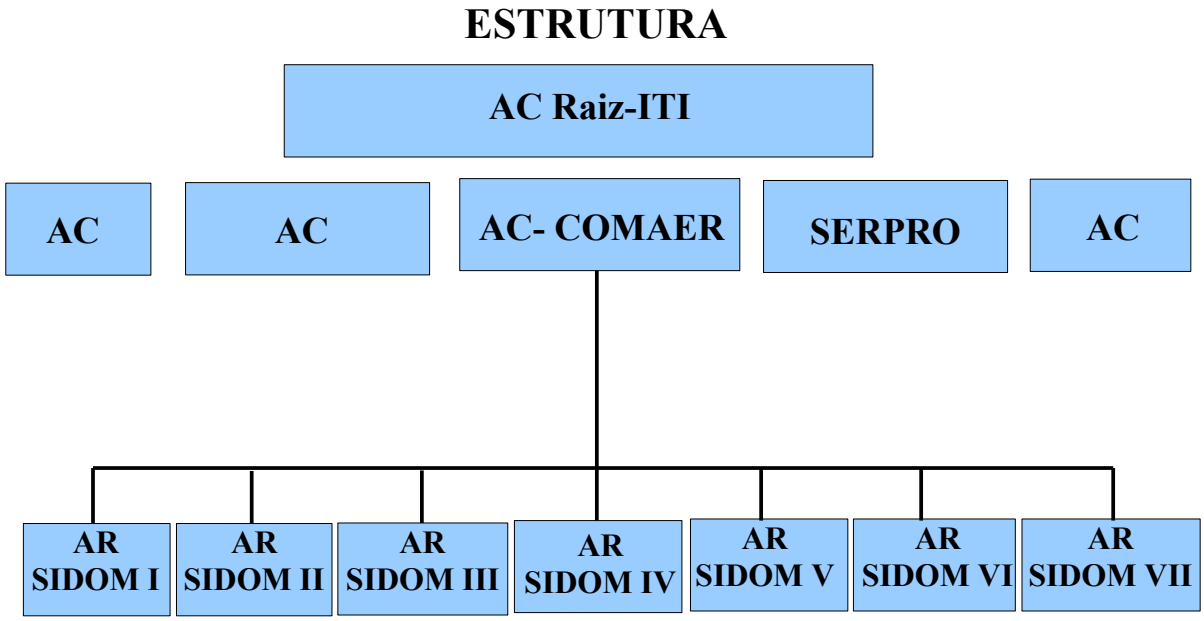


Figura 13: Estrutura da certificação do COMAER.
Fonte: Autor.

Esta arquitetura deu-se em virtude de que as SIDOM (Seções de identificação de Organizações Militares) serem seções já existentes dentro do organograma do Comando da Aeronáutica e hoje responsáveis pela emissão e credenciamento dos militares por meio da identidade funcional.

Alicerçado principalmente pelo projeto da identidade digital, projeto este que já toma vulto na esfera do governo Federal apoiados principalmente pala Aeronáutica e a Polícia Federal, é que foi escolhida a SIDOM como autoridade de registro da AC COMAER, as quais passarão da emissão da tradicional cédula de identidade as quais conhecemos para a identidade digital que conterá um chip com a assinatura do militar integrante da força, proporcionando este a assinar qualquer documento com sua própria identidade além de outros projetos que virão alicerçado a identidade funcional.

Claro é que no primeiro momento deveremos equipar e treinar os integrantes das SIDOM´S para isso e as primeiras assinaturas serão distribuídas em toquem, bem como a primeira SIDOM escolhida para emissão de um certificado será a SIDOM VI, no VI COMAR em Brasília que estará amparada pelo o CCA-BR e que deverá operar com seus trabalhos rotineiros em um local físico no prédio do

Comando da Aeronáutica até que sejam capazes de realmente exercer sua atividade sem o apoio daquele órgão técnico desenvolvedor.

Figura 14: Identidade Digital.
Fonte: Projeto identidade digital do COMAER.

Por definição ainda terá que ser citado o certificado digital como sendo o documento eletrônico de identidade emitido pela AC COMAER credenciada pela Autoridade Certificadora Raiz da ICP-Brasil – AC Raiz.

O usuário será o militar integrante da Força titular de Certificado Digital, bem assim de qualquer outro certificado digital emitido por Autoridade Certificadora habilitada e credenciada pela ICP Brasil.

3.2 SOLICITAÇÃO DE CERTIFICADO

O militar interessado na obtenção de um certificado digital deverá escolher uma das Autoridades de Registro Habilitadas, que no referido caso serão as Seções de Identificação (SIDONS), dos Comandos Aéreos Regionais, munidos do documento de identidade funcional, CPF, e o comprovante de residência, efetuar o preenchimento de uma solicitação e aguardar o cadastro para a emissão do certificado.

Não poderão ser titulares de certificados, as pessoas físicas cuja situação cadastral perante o CPF esteja enquadrada na condição de cancelado.

3.3 RENOVAÇÃO DE CERTIFICADO

O pedido de renovação de um certificado deverá ser feito dentro do seu período de validade do certificado existente.

O militar usuário interessado na renovação deverá solicitar, por meio de sua assinatura eletrônica, na página da autoridade certificadora, na rede interna do COMAER (Intranet), a renovação do certificado, o qual será processado e emitido eletronicamente de imediato.

3.4 REVOGAÇÃO DE CERTIFICADO

Revogar um certificado digital da AC COMAER implica em torná-lo inválido, impossibilitando, a partir da revogação, o seu uso. Para revogar seu certificado digital, o militar usuário do certificado deverá acessar a página de revogação da Autoridade Certificadora da AC COMAER, por meio da rede interna (intraer) Habilitada, emissora do Certificado Digital, preenchê-la com os dados solicitados, solicitando a sua revogação.

Haverá casos em que a Seção de Pessoal militar de cada organização a que o militar está subordinado deverá tomar a frente dessas ações uma vez que podemos deparar com o militar pedindo baixa das fileiras da Força e no ato da devolução de sua identidade o mesmo será submetido ao pedido de revogação de sua assinatura digital.

Estas ações ainda apesar de definidas e constarem de documentos em fase de elaboração poderão sofrer modificações as quais atenderão e buscarão uma melhor eficiência do processo e sua otimização.

Por exemplo é perfeitamente possível que a revogação do certificado digital do militar esteja vinculado ao SIGPES que uma vez alimentado com informações de desligamento ou afastamento do militar das fileiras da força transmita eletronicamente o pedido de revogação de seu certificado a autoridade de registro ou a AC COMAER que providenciará sua revogação.

Neste capitulo foi possível entender a estrutura que esta definida para AC COMAER justificada pela visão prospectiva de outros projetos que virão alicerçados nos que já são realidade e farão parte de um sequenciamento, ou melhoramento dos serviços disponíveis aos usuários, não só do COMAER e do Ministério da Defesa mas também ao cidadão Brasileiro. Isso é comprovado quando se verifica o interesse e a parceria que a Polícia Federal propôs a força no desenvolvimento da identidade digital, objeto já presente em países como Espanha.

Desta forma será visto a seguir a comparação entre modelos de certificação digital adotados em outros continentes e países que vem a corroborar com a certeza de que nossa estrutura digital está em um padrão de excelência com o resto do mundo sem os problemas que eles já enfrentam por terem sido os desbravadores desta nova tecnologia.

3.5 COMPARAÇÕES ENTRE MODELOS

O Brasil possui uma inserção que pode-se chamar de tardia no mundo da certificação. Se esse fato, em alguns casos, pode levar a um entendimento de dificuldades, concorrências ou mesmo uma inserção subordinada a modelos solidários, não é o que aconteceu na certificação digital.

A seguir serão descritos modelos de infraestrutura de certificação digital de alguns países para que ao final do capítulo possamos realizar uma comparação com o implantado no Brasil.

3.6 MODELO AMERICANO

Segundo Lino Sarlo (2004) 309 os Estados Unidos possuem mais de uma infraestrutura de chaves públicas e sua implementação foi regida por uma forte influência do mercado, que inicialmente ditou as regras e a velocidade de implementação. Se por um lado essa situação constituiu uma vanguarda mundial, por outro lado trouxe consigo uma dificuldade inerente a padronização e interoperabilidade do sistema.

Partindo-se do princípio que a interoperabilidade de soluções é um ponto de partida crucial para o fortalecimento de uma infraestrutura, o que se dizer da convivência e interoperabilidade de várias infraestruturas com diferentes formas de gestões, tendo que se relacionar de forma harmoniosa e eficaz entre si?

Como fazer para um certificado emitido por uma infra-estrutura, que possuía forte presença no lado oeste do país, fosse válido e reconhecido com valor legal quando utilizado em serviços sobre soluções de outra infraestrutura?

[6]Os EUA necessitaram perseguir e implementar um modelo que contemplasse a solução desses problemas. A estrutura criada exerce a função de cadeia de certificação cruzada (*Cross Certification*). Ela atua como um concentrador da certificação e traz, de uma forma inerente, a figura do agente de validação. É ele que dá o caráter legal à certificação cruzada.

[7]A seguir é apresentada uma descrição, que permite uma melhor visualização do modelo.

3.6.1 DESCRIÇÃO

Fase 1: Inicialização

---

[6] SILVA, Lino Sarlo da. Public Key Infrastructure PKI. 1 ed. São Paulo: Novatec, 2004.

[7] LENOTTI, José Roberto. Infraestrutura de Chaves Públicas, um estudo comparativo entre o modelo brasileiro e o modelo americano. São paulo: Faculdade de Ciências da Unesp, 2002.

a) a infraestrutura requer da *US Government's Federal Bridge Certification Authority* (FBCA) a certificação cruzada;
b) inicia-se a revisão dos aspectos técnicos e da política de certificação da Infraestrutura de chaves pública;
c) determina-se se a aplicação está em total conformidade com as regras;
d) verifica a aplicação e se está apropriada com a certificação cruzada; e
e) o órgão federal de certificação dos EUA toma a decisão se a ICP em questão está apta a passar para a próxima fase de habilitação.

Fase 2: Mapeamento da política de certificação do órgão que pleiteia
a) mapeamento da política de certificação; e
b) avaliação do órgão de auditoria e conformidade.

Fase 3: Interoperabilidade Técnica
a) nessa fase, são realizados todos os testes de interoperabilidade, em cima de um protótipo, visando resolver todos os problemas de incompatibilidade entre a tecnologia da ICP e os produtos já avaliados que compõem outras ICP, visando diminuir o risco de introdução de um novo certificado junto as ICP que estão em conformidade e em produção.

Fase 4: Acordo entre as partes
a) o órgão federal dos EUA, autoridade responsável pela certificação digital, toma a decisão de agregar a nova ICP; e
b) é negociado um acordo de certificação cruzada, nos termos da *US Government's Federal Bridge Certification Authority (FBCA).*

Fase 5: Manutenção
a) revisão periódica da conformidade;
b) resolução de problemas encontrados;
c) eventuais mudanças de gestão; e

d) renovação ou término de acordo de certificação cruzada.

Observa-se que os aspectos acima tratados dizem respeito apenas a certificação cruzada por conta da interoperabilidade devido à existência de várias ICP. Trata-se, não da atuação da autoridade federal de certificação, mas da autoridade de certificação cruzada, havendo um verdadeiro *over head* operacional no modelo usado nos EUA.

O caso americano é um caso onde os *players* da certificação se apresentam antes da conformidade do modelo, quando isso ocorre há a necessidade de se tratar um extenso legado já estabelecido.

Observa-se agora o caso Espanhol, onde outras dificuldades se apresentam.

Figura 15: Modelo Americano.
Fonte: Autor.

3.7 MODELO ESPANHOL

[8]A Espanha é um pais que tem feito um forte investimento em certificação digital. O principal *player* do setor tem sido a *Real Casa de Moneda de Espanha*, através do projeto [9]CERES. No entanto outras ICP estão estabelecidas, gerando alguns problemas de gestão de modelo.

Se por um lado a *Casa de Moneda de Espanha* é a grande autoridade certificadora, por outro lado a identidade eletrônica é o grande propulsor da certificação digital naquele país. Ocorre que a carteira de identidade eletrônica, com o uso de *targetas digitales* e com certificados, é um programa que pertence a uma outra ICP estabelecida dentro do Ministério do Interior.

Os problemas na gestão da conformidade e da integração se apresentam dentro da própria estrutura de Estado/governo. Ocorre que também existem outras autoridades certificadoras privadas, criando uma verdadeira miscelânea de ICP.

O governo Espanhol está atento para essa situação e, como o CERES é o grande fomentador do negócio de certificação espanhol, há uma tendência de que este se fortaleça como autoridade certificadora raiz, ou mesmo comece a exercer a função de autoridade de certificação cruzada. De todo modo, algo deverá ser feito, visando dar integração aos certificados emitidos por aquele pais.

3.8 MODELO ALEMÃO

O modelo Alemão[10] está baseado em uma infraestrutura descentralizada, tendo como autoridade certificadora raiz a Agência Reguladora para Telecomunicação e Correios, Regulierungsbehoerde für Telekommunikation und Post (ReGT)[11].

---

[8] EMBAIXADA DA ESPANHA. **Infra estrutura de chaves públicas da espanha.** Brasília, DF, 2004. 23 dispositivos, colorido.

[9] CERES – *Certificación Española* (Projeto de Certificação Digital da Espanha)

[10] EMBAIXADA DA ALEMANHA. **Infra estrutura de chaves públicas alemã.** Brasília, DF, 2004. 18 dispositivos, color.

[11] Regulierungsbehoerde für Telekommunikation und Post (ReGT) - Agência Reguladora para Telecomunicação e Correios (autoridade certificadora raiz).

Seu modelo, formulado através da lei Signaturgesetz (SigG)[12], aprovada pelo parlamento alemão (Bundestag) em 13 de junho de 1977, que por sua vez faz parte de uma lei mais ampla, a lei de serviços de informação e comunicação, Informations und Kommunikationsdienste gesetz (IuKDG)[13], concedia inicialmente autorização somente para Agência governamental voltada para a segurança da informação, Bundesamt für Sicherheit in der Informationstechnik (BSI)[14], funcionar como autoridade certificadora.

O objetivo principal desta lei é estabelecer as condições para o uso seguro da assinatura digital, porém é uma lei técnica, não trata a validade legal da assinatura digital, como por exemplo no Japão,na Malásia e em Singapura.

Porém, visando a melhora do modelo inicialmente utilizado, o governo alemão descentralizou sua estrutura e credenciou um grupo fechado de entidades públicas e privadas para exercerem o direito de emissão de certificados digitais além de estarem credenciadas para supervisionar e fiscalizar o cumprimento da lei de normatização de seu modelo.

Hoje em dia, a concessão de entidades privadas no âmbito da certificação digital é visto naquele país como um ponto forte no sentido de adoção e cumprimento da lei. Ela contribui para solidificação e modificação de uma cultura voltada para a nova tecnologia.

3.9 MODELO DA COMUNIDADE EUROPÉIA

Com a criação da Comunidade Europeia, vários problemas surgiram e estão sendo resolvidos depois de muitas reuniões com os diversos países. Um deles é o modelo de certificação digital a ser adotado para a Comunidade Europeia.

Porém, ainda sem um consenso geral, a estratégia utilizada está direcionada para uma proposta voltada a unificação dos diversos modelos já existentes e praticados nos países europeus.

---

[12] Signaturgesetz (SigG) - lei subsidiária da lei IuKDG, define as normas de certificação digital no pais.

[13] *Informations- und Kommunikationsdienste- Gesetz (IuKDG)* - lei de serviços de informação e comunicação, superior a SigG define as diretrizes da certificação digital na Alemanha.

[14] Bundesamt für Sicherheit in der Informationstechnik (BSI) - Agência governamental de segurança da informação.

3.10 BENEFÍCIOS DA UTILIZAÇÃO DA CERTIFICAÇÃO DIGITAL

As possibilidades de aplicação da assinatura digital, com uso do certificado digital, são muito amplas. Dentre elas podemos citar algumas como: comércio eletrônico; processos judiciais e administrativos, assinatura da declaração de imposto de renda, apresentação de projetos de lei por iniciativa popular, serviços cartoriais como obtenção e envio de documentos e certidões; transações seguras entre instituições financeiras; identificação de sítios na rede mundial de computadores e vários outros serviços prestados, que hoje existem e que aparecerão em futuro próximo.

Não há duvida de que a certificação digital permitirá a expansão e um fortalecimento das relações nesse novo setor, conhecido como economia digital.

O e-comércio, como são conhecidas as transações de compra e venda realizadas pela internet, será também um dos grandes beneficiários do uso da assinatura digital, sendo um incentivador e precursor bastante interessado desta nova tecnologia e de sua constante otimização.

Sabe-se que uma das fortes tendências do comércio eletrônico é a integração e customização dos serviços aos clientes. O cliente cada vez mais exige um serviço consistente e seguro. Se fosse possível visualizar o consumo de uma sociedade daqui a cinco anos, se veria uma mudança significativa da participação da economia digital no chamado *market share*.

A conveniência oferecida pela economia digital será transformadora de hábitos e se estabelecerá culturalmente. Hoje há setores em que os índices de utilização de um canal eletrônico já supera o pessoal.

O caso do setor bancário já se torna efetivamente um paradigma, pois o número de transações realizadas em máquinas de alto atendimento, já supera em muito as transações realizadas pessoalmente na boca do caixa. Agrega-se a isso as operações realizadas pela máquina administrativa do governo, onde uma significativa parcela do PIB brasileiro transita através de uma rede de computadores, tornando assim esta tecnologia não um artigo de luxo supérfluo, mais sim uma necessidade absoluta que veio para ficar e otimizar, dando transparência, lisura e agilidade às negociações.

Segundo dados da câmara e-net em outubro de 2006, apenas três dias foram suficientes para serem realizados mais de 4 milhões de transações relacionadas a vendas seguras utilizando a certificação.

Agregar segurança a uma transação está diretamente ligada ao valor de seu produto e ao serviço disponibilizado.

Quando são analisadas todas estas melhorias proporcionadas pela certificação digital no meio civil, pode-se prospectar as vantagens que trará para o Comando da Aeronáutica.

3.11 CERTIFICAÇÃO DIGITAL NO COMAER

A demanda pela utilização dos benefícios providos pela infraestrutura de chaves Públicas (Integridade, Autenticidade, Sigilo e Irrefutabilidade) em diversos setores do COMAER tem sido identificada como uma ferramenta necessária que otimizará a administração interna.

O CCA-BR hoje é constantemente consultado quanto a um cronograma de implantação desta tecnologia no âmbito de todo o COMAER. Porem também hoje identifica-se várias organizações tomando iniciativas próprias na busca de soluções e tendendo a contratar serviços de terceiros para atender às necessidades da área de negócio, tais como SDPP, SEFA e CABW.

Vários são os casos de sucesso com o uso de certificação, trabalhando os aspectos anteriormente já citados neste trabalho.

Quando o assunto é controle, a rastreabilidade permite aos agentes de controle um perfeito acompanhamento de ações e atividades. Além dessa rastreabilidade, existe a questão da responsabilidade legal dos atos administrativos, que são de extrema importância na construção da conformidade legal. Nesses casos, temos uma perfeita identificação dos autores, além da segurança inerente do uso do certificado.

Na questão facilidade, pode-se ainda citar a utilização da tecnologia na consulta e recebimento autenticado do contracheque pela internet, contribuindo para agilizar a consulta, bem como o recebimento do documento.

Outra possibilidade bastante discutida e já em estudo seria o uso da certificação digital pelos oficiais de saúde, oportunidade na qual ter-se-ia todos os prontuários sendo assinados digitalmente e transitando pela rede interna da Aeronáutica, podendo ser acessada por qualquer médico em qualquer hospital da Força Aérea.

Nas transações financeiras, ter-se-á a perfeita integração com os serviços reguladores do Governo Federal (SIAFI, SIAPE, etc), adequando-se às exigências já impostas pelo governo federal.

Inicialmente, é fácil constatar que menos papel gera maior eficiência e controle, contribuindo assim para uma administração mais simples e transparente.

3.11.1 BENEFÍCIOS NO EMPREGO MILITAR

É no campo do emprego militar que a inserção da certificação digital talvez traga os maiores benefícios para atividade fim da Força. A confiabilidade e o sigilo na transmissão dos dados, proporcionarão, aliada a rapidez do método, uma agilidade nos processos e, em consequência, uma abreviação no tramite decisório. Neste contexto, ordens veiculadas pelo comando e controle da Força, passarão a estar menos vulneráveis quanto a transmissão de dados. Como exemplo, pode-se citar a divulgação e distribuição de ordens de operações e toda documentação pertinente a manobras ou exercícios operacionais para as Unidades envolvidas.

Outro campo onde o método poderá trazer ganhos substanciais, refere-se à transmissão e recebimento de mensagens rádio. As estações rádio possuem ainda importância vital no sistema de comunicações, principalmente, em caso de contingência numa possível falha operacional da rede de computadores. Porém, a tendência, em um futuro próximo, é a total dependência dos meios de informática para a transmissão de dados. No caso das mensagens rádio, a confiabilidade e a segurança que o sistema proporciona irão diminuir substancialmente o trânsito de papel no Comando da Aeronáutica.

3.12 PROJETOS EM ANDAMENTO

A Tecnologia da Informação por meio de sua acelerada evolução tem apontado tendências e demonstrado interesse na tecnologia *Smart Card* que tem crescido a uma taxa elevada nos últimos anos. O número e a variedade de aplicações baseadas em *Smart Card* em diversos setores vêm demonstrando sua importância e a sua consolidação.

Entre os fatores que levaram ao crescimento do interesse nessa tecnologia incluem-se o declínio no seu custo de fabricação e a crescente preocupação com a limitação dos cartões de tarja magnética e suas brechas de segurança nos sistemas em que são utilizados, além, é claro, de dificultar as falsificações de cartões de serviços, como por exemplo o SARAM, carteira de identidade, e outros documentos.

Neste contexto que as vantagens da utilização de uma nova cédula de identidade (carteira digital) no âmbito do COMAER, adequando às tecnologias atuais, diminuindo radicalmente os custos na emissão, facilitando o controle e unificando a quantidade de cartões confeccionados por diversos setores, tem tomado vulto.

Assim o Projeto Identidade Multifuncional tem por fim o estabelecimento do processo de identificação com uma mídia única, com disponibilidade de duas tecnologias embutidas: a de chip de contato (*Smart Card*), e certificação digital, garantindo a operabilidade da autoridade certificadora do COMAER, e viabilizando a interação de sistemas na área da TI.

3.12.1 IDENTIFICAÇÃO DA CARÊNCIA OPERACIONAL

a) Identidade atual possui apenas três itens de segurança (talho doce, fundo numismático e palavra AER), o que facilita a falsificação de documentos;
b) Número excessivo de modelos de cédulas de identidade, dificultando o controle;
c) Legislação dos Processos de Identificação desatualizada;

d) Existência de “espelhos” de identificação em 27 localidades do COMAER, espalhadas por todo o Brasil, aumentando a probabilidade de falsificações da carteira de identidade, devido à facilidade atual de impressão de documentos;
e) Diversidade de cartões de acesso em uso no COMAER;
f) Despadronização e desatualização de tecnologias de acesso (código de barras, magnético, *wiegand*, proximidade passivo etc.);
g) Inexistência de um cartão para certificação digital, pois com o projeto da Autoridade Certificadora do Comando da Aeronáutica, atualmente sob responsabilidade do Centro de Computação da Aeronáutica de Brasília, cada militar ou civil, da ativa ou reserva, que necessitem tramitar documentos eletrônicos, assinados digitalmente, deverão possuir uma mídia para carregar as chaves da assinatura digital, originadas por essa Autoridade;
h) Necessidade de criação de um método de controle dos comensais (DIRINT/SDAB), onde o usuário do rancho não necessitará mais preencher livros, pois o registro da presença será automático;
i) Necessidade de criação de um sistema de venda de fardamento para maior controle desse material;
j) A não validade jurídica da carteira de identidade.
k) A necessidade de substituição dos cartões de atendimento hospitalar (SARAM) nos Hospitais do COMAER, aumentando o controle no atendimento dos usuários do Sistema de Saúde da Aeronáutica (SISAU).

3.12.2 CENÁRIO

Devido à solicitação, da SDAB, de aquisição de roletas e cartões de controle de acesso para serem utilizados no módulo de controle de comensais (SISUB), o Exmo. Sr. Comandante -Geral do Pessoal vislumbrou a possibilidade desse cartão também atender a necessidade de um novo cartão de identidade para

o pessoal do Comando da Aeronáutica. Com isso, a ideia é substituir os diversos cartões de controle de acesso e utilização de serviços no âmbito do Comando da Aeronáutica por um cartão único.

Devido à facilidade de falsificação dos documentos atuais, como: identidade, por apresentar somente três itens de segurança, sendo que as tecnologias atuais dispõem de maior quantidade desses quesitos; o cartão de atendimento hospitalar (SARAM), por não apresentar itens de segurança, facilitando a tentativa de fraude nos atendimentos; e, por último, o acesso a armamentos, devido às últimas tentativas de desvio de material militar, por parte de pessoas mal intencionadas, mostrando a necessidade do aumento do controle de acesso a esses equipamentos. Em face do exposto, faz-se necessário a utilização de cartões com tecnologias de segurança mais robustas, os quais se encontram disponíveis no mercado.

Utilização da assinatura digital em documentos eletrônicos, que será necessária para a implementação do projeto da Autoridade Certificadora do Comando da Aeronáutica, sob responsabilidade do Centro de Computação da Aeronáutica de Brasília, fornecendo suporte jurídico, através da legalidade do ato administrativo para o projeto do Sistema Informatizado de Gestão Arquivística e Documentos da Aeronáutica (SIGADAER).

Possibilidade na utilização de diversos sistemas de informação que requeiram validação jurídica do ato administrativo, tais como: o boletim no Sistema de Informações Gerenciais de Pessoal do Comando da Aeronáutica (SIGPES), o Sistema de Avaliações de Oficiais e Graduados, junto às suas respectivas Comissões (Comissão de Promoções de Oficiais e Comissões de Promoções de Graduados) e etc.

Aproveitamento do cenário político atual para despontar o Comando da Aeronáutica como órgão inovador, na Administração Pública Federal, para junto com o Instituto Nacional de Identificação, órgão da Polícia Federal, integrar, mantendo a autonomia dos dados do Sistema de Identificação da Aeronáutica atual (SIDENT), com o Projeto do Registro de Identificação Civil (RIC), o qual produzirá um documento de numeração única no país junto aos Estados da Federação. Até 2017

(dois mil e dezessete) todo cidadão brasileiro deverá estar com o seu RIC atualizado.

Possibilidade de informações emergenciais para atendimento médico da pessoa que possuir o cartão, tais como tipo sanguíneo, doenças patológicas, alergias a alimentos e ou a medicamentos específicos e etc.

Possibilidade das equipes de serviço, nos portões da guarda, em todas as OM do Comando da Aeronáutica, possuírem leitores biométricos para validação do portador da cédula de identidade.

Uma das formas de emprego do cartão multifuncional. seria como dinheiro eletrônico, através da compra de fardamento com autenticação digital, sendo diretamente descontada na folha de pagamento do militar.

O cartão armazenará todos os dados sobre a saúde do usuário (últimas consultas, doenças, plano de saúde), facilitando o gerenciamento do atendimento.

3.13 CONCEPÇÃO DE EMPREGO

Antes de descrever a concepção de emprego da tecnologia, faz-se necessária a explicação do que é a tecnologia proposta, o que dará base teórica fundamental ao entendimento do emprego nos diversos cenários descritos no item 9.1 desta dissertação.

3.13.1 CARTÕES INTELIGENTES

A tecnologia *Smart Card* consiste num cartão plástico com um *chip* que contém memória e em alguns modelos possui um microprocessador, ROM e sistema operacional (próprio de cada fabricante). A capacidade dos cartões é bem variada conforme o *chip*, o fabricante e o tipo de aplicação, indo de alguns *bytes* até alguns *Kylobytes*.

O *Smart Card* foi inventado nos anos 70 na França, onde se espalhou pela Europa. Aos poucos, esta tecnologia está sendo utilizada no mundo inteiro. No Brasil, as aplicações com *Smart Card* começaram em meados de 1995 e atualmente existem vários projetos em operação.

3.13.1.1 Tipos de Arquitetura:

Cartão de Memória:

São cartões de armazenagem de informações e dependendo da tecnologia empregada, podem ser descartáveis ou reutilizáveis. Os cartões de memória possuem as seguintes características:

a) Nível de segurança básico;

b) Cartões utilizados para uma única aplicação; e

c) Utilizado para aplicações mais simples, por exemplo : telefonia.

Cartão com Microprocessador:

Este tipo de cartão é o "verdadeiro" Smart Card, pois contém uma CPU além da área de memória. Os cartões microprocessados possuem as seguintes características:

a) Nível de segurança maior;

b) Podem ser com contato, sem contato, ou combinados;

c) Comporta mais de uma aplicação.

3.13.1.2 Tipos de Interface:

Cartões com Contato:

O acesso aos dados e aplicações do *Smart Card* se dá através de contato físico com o dispositivo de leitura. Exige que o cartão seja inserido no dispositivo. Atualmente seu uso está direcionado a cartões de fidelidade e de crédito.

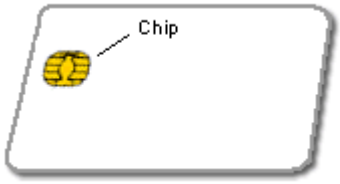


Figura 16: Cartão com contato
Fonte: Curso de Certificação Digital

Cartões sem Contato (*Contactless*):

O acesso aos dados e aplicações acontece sem contato físico entre o *chip* e o dispositivo de leitura através de rádio-frequência. São utilizados para aplicações cujas transações devem ser rápidas (ex.:controle de acesso, transporte público e pedágios).

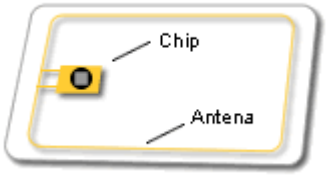


Figura 17: Cartão sem contato
Fonte: Curso de Certificação Digital

Cartões Combinados e Cartões Híbridos

Estes cartões combinam os dois tipos de interface, visando à integração de aplicações de contato e sem contato em um mesmo cartão. Diferem pelo fato de os cartões combinados possuírem uma área de memória em comum, enquanto os cartões híbridos simplesmente têm o mesmo *chip*. Visa integrar as aplicações de contato e sem contato em um mesmo cartão.

3.13.2 PADRONIZAÇÃO ISO

O tamanho do cartão é determinado pelo padrão internacional ISO 7816. Este padrão define também as características físicas do plástico, incluindo faixa de temperatura, flexibilidade do cartão, posição dos contatos elétricos e como o microchip se comunica com o mundo exterior.

a) ISO - 7816-1: Características físicas (tamanho do cartão, etc.) - com contato;
b) ISO - 7816-2: Dimensão e local dos contatos no cartão - com contato;
c) ISO - 7816-3: Protocolo de sinais e transmissão - com contato;
d) ISO - 7816-4: Formato dos comandos de acesso ao cartão - com contato; e
e) ISO - 10536 : Para a parte sem contato.

3.13.3 VANTAGENS DO *SMART CARD*

a) Pode conter várias aplicações diferentes;
b) As transações são feitas de forma *off-line*;
c) O próprio cartão autoriza a transação, uma vez que todas as informações necessárias estão contidas nele;
d) Segurança alta - criptografia na autenticação;
e) Dificuldade na duplicação de um cartão (evita fraudes);
f) Vida útil longa (10 anos);
g) Maior robustez em relação aos agentes externos; e
h) Aplicações com *Smart Card*.

3.13.4 DETALHES TÉCNICOS DO *SMART CARD*

Cartões por contato físico - Os cartões não possuem bateria, sendo que a energia é totalmente fornecida pelo leitor. As normas ISO/IEC 7816 e ISO/IEC 7810 definem, para esta categoria de Smart Cards, os seguintes requisitos:

a) o formato físico;
b) a posição e o formato dos conectores elétricos;
c) as características elétricas;
d) os protocolos de comunicação;
e) o formato dos comandos enviados ao cartão e as respostas retornadas por ele;
f) a robustez do cartão; e
g) a funcionalidade.

Por contato físico, entende-se a inserção do cartão na leitora, onde os contatos dos terminais do cartão com os da leitura, permitem a troca de dados entre ambos. É importante salientar que todos *Smart Cards* possuem terminais para este tipo de conexão.

A segunda classe se refere aos cartões que não necessitam de contato físico com a leitora, o que indica que a conexão é feita através de ondas

eletromagnéticas. A ausência do ato de inserção traz benefícios como economia de tempo e não desgaste dos terminais do cartão.

Por serem muito mais baratos, os cartões por contato ainda são os mais utilizados, oferecendo um nível razoável de segurança e abrangendo uma ampla gama de aplicações. Os cartões por contatos são também chamados *Memory Cards* ou Cartões Memória.

Os *Smart Cards* que não fazem uso de contato físico são tipicamente *Microprocessor Cards* ou Cartões Microprocessados. Embora não seja do escopo dos cartões de identificação, a modalidade de transmissão sem contato permite que o cartão propriamente dito seja apenas um portador do *chip*.

Cartões sem contato físico - *Smart Cards* sem contato possuem um *chip* que se comunica com o leitor através de RFID, com taxas de transmissão de 106 a 848 Kb/s. Tais cartões exigem somente uma proximidade a uma antena para a transação de dados. São geralmente utilizados quando a transação deve ser feita rapidamente e com as mãos livres, como em sistemas de trânsito.

A norma ISO para tal tecnologia é a ISO/IEC 14443 (2001). Ela define dois tipos de Smart Cards sem contato (categoria A e B), permitindo comunicação a distâncias de até 10 cm. Existem propostas para as categorias C, D, E e F, que foram rejeitadas pelo comitê de padronização. Uma alternativa é a ISO 15693, que permite comunicações à até 50cm (ideal trabalhar com distâncias até 7cm).

3.13.5 CARACTERÍSTICAS DOS SMART CARDS

a) Custo - A faixa de preço típica varia de US$7,00 a US$10,00. O custo aumenta à medida que maior capacidade de armazenagem e de processamento é acrescentada ao chip e esse custo diminui à medida que o volume de produção aumenta.
b) Confiabilidade - É garantido 10.000 ciclos de leitura/escrita. Os cartões devem atender as especificações da ISO (*International Standards Organization*) e passar por uma bateria de testes que abrangem: testes de torção, de flexibilidade, de desgaste, de concentração de carga, temperatura, umidade, eletricidade estática, ataque químico,

ultravioleta, raio X e testes de campo magnético.

c) Correção de Erro - O Sistema Operacional do Chip (COS - Current Chip Operating Systems) realiza seu próprio algoritmo de correção de erro. O sistema operacional do terminal deve checar os dois bytes de código de Status que o COS retorna após receber o comando do terminal (como definido na ISO 7816 Parte 4 e nos comandos proprietários). Dessa forma o terminal toma as ações corretivas necessárias.
d) Capacidade de Armazenamento - A memória mais usadas nos Smart Cards são as EEPROM (Electrically Erasable Programmable Read-Only Memory) que possuem capacidade de 8K - 128K bit. (1Kbits armazena algo em torno de 128 caracteres, o equivalente a uma frase de texto. Entretanto, com as modernas técnicas de compressão, a quantidade de informação armazenada em um Smart Card pode ser significativamente expandida).
e) Segurança - Smart Cards são altamente seguros. As informações armazenadas no chip são difíceis de serem copiadas ou alteradas, ao contrário dos cartões de tarja magnética que podem ser facilmente clonados. O microprocessador e o coprocessador do chip suportam criptografia, autenticação e assinatura digital para não-repúdio.
f) Capacidade de Processamento - Cartões mais antigos usavam um micro controlador de 8-bits com clock de 16 MHz. Os cartões mais modernos utilizam um micro-controlador RISC de 32-bits rodando a um clock de 25 a 32 MHz, com um coprocessador para a criptografia.

3.13.6 MEMORY CARDS OU CARTÕES MEMÓRIA

Do ponto de vista da aplicação, estes cartões por contato podem ser vistos como uma memória programável. Assim, as informações contidas no *Smart Card* podem ser apagadas e reescritas inúmeras vezes. Esta característica faz destes cartões um bem "reciclável" quando comparados aos cartões magnéticos.

Embora existam diversas formas de disposição, o espaço de endereçamento da memória é linear, com possíveis faixas para uso relacionado à segurança.

Há no mercado atual, *Memory Cards* com capacidades que vão de 1 a 64 Kbits e recursos que abrangem criptografia. Essas inovações tecnológicas sucederam uma vertente dos *Memory Cards*, os *Logic Cards* (Cartões Lógicos).

Assim, os 1024 *bytes* (8 *Kbits*) de memória deste cartão estão dispostos em três áreas:

a) Área do fabricante, onde estão gravadas informações acerca do modo operacional do cartão, dados de identificação do fabricante, etc;
b) Área de aplicação, onde os dados da aplicação podem ser lidos ou escritos;
c) Área de segurança, na qual são armazenados alguns dados que permitem que o cartão seja acessado somente pelo seu proprietário.

3.13.6.1 *Smart Cards* Microprocessados

Um *Smart Card* Microprocessado possui os principais elementos de um computador, como uma CPU (Central *Processing Unit*), um sistema de memórias e barramentos de entrada e saída. Um sistema operacional, gravado no cartão, permite que uma comunicação em alto nível possa ser estabelecida com a leitora a que está conectado.

O sistema de memórias do *Smart Card* Microprocessado possui 3 tipos de memórias: ROM (*Read-Only Memory*), EEPROM (*Electrically Erasable Programmable Read-Only Memory*) e uma pequena quantidade de RAM (*Random Access Memory*). A ROM é onde o sistema operacional do *Smart Card* é armazenado e não pode ser alterada. Na EEPROM são armazenados os dados da aplicação, isto é, ela pode ser lida e escrita por aplicativos. Os dados presentes nessa memória podem permanecer, se não sobrescritos, por até 10 anos. Entretanto, a EEPROM possui 2 inconvenientes:

a) Lentidão. Leva-se de 3 a 10 ms para se escrever nessa memória;
b) Número de regravações. Chega-se a no máximo 100.000 gravações.

A RAM, por ser escassa, é o recurso mais precioso do cartão do ponto de vista do desenvolvedor. Além disso, ela não é usada somente pela aplicação, mas também por rotinas operacionais.

Antigamente a CPU era um microcontrolador de 8 bits, tipicamente utilizando o conjunto de instruções dos chips Motorola 6805 ou Intel 8051 a um clock de 16 MHz. Atualmente ela é um microcontrolador RISC de 32 bits atingindo um clock de 25 a 32 MHz. As suas instruções manipulam também os endereçamentos de memória e dos registradores e operações de entrada e saída. Alguns fabricantes implantam instruções próprias para um uso específico.

A crescente demanda por criptografia, exige cada vez mais poder de processamento da CPU. Um processo de decriptação RSA 1024 bits, por exemplo, pode demorar até 10 segundos. Assim, alguns fabricantes embutem coprocessadores no cartão, a fim de acelerar esse serviço.

O canal de entrada e saída do *Smart Card* é serial e unidirecional. Isto significa que os *bits* passam um a um em um único sentido de fluxo por vez. O hardware do *Smart Card* permite velocidades de até 115.200 bps.

A comunicação entre o cartão e o software de aplicação é do tipo mestre (*software*) e escravo (cartão). O software envia comandos ao cartão e espera por uma resposta. O cartão nunca envia dados ao software exceto em resposta a um comando.

Os sistemas operacionais dos *Smart Cards* suportam dois tipos de transferência: por caractere ou por bloco. A transferência por caractere ocorre quando os dados são transferidos caractere a caractere até formar uma palavra. Já na transferência por bloco, são transmitidos quadros inteiros por vez, o que faz deste tipo de transferência mais complexo que o outro.

Para o Projeto Identidade Multifuncional, haverá a necessidade do desenvolvimento de aplicações informatizadas com funcionalidades específicas para integrar os dados coletados pelo kit de captura, e a base de dados existente no atual Sistema de Identificação da Aeronáutica. Devido a essa necessidade de aplicação, torna-se vital a compreensão da interação da biometria com *Smart Cards*.

3.13.7 BIOMETRIA E SMART CARDS - CARACTERÍSTICAS FÍSICAS COMO SENHAS

Biometria é a tecnologia de captura e armazenamento de características humanas únicas que tem o propósito de reconhecimento e verificação de identidade.

As características Biométricas são divididas conceitualmente em dois segmentos:

a) Características físicas: característica facial, leitura digital, geometria da mão e olhos (íris, retina);
b) Características comportamentais: verificação de voz, movimentação labial, assinatura dinâmica e velocidade de digitação.

3.13.7.1 Autenticação de usuário

Características biométricas estão sendo utilizadas em muitas aplicações de autenticação de usuários e é baseada em algo que o usuário sabe, tais como PIN ou senha, ou algo que ele tem, tal como um cartão inteligente ou um outro token. Sistemas biométricos trabalham com relacionamento das características físicas - algo que é único e inseparável para a pessoa.

PINs, senhas e chaves podem ser esquecidas, perdidas ou roubadas, biometria não pode. A anatomia do usuário traz o significado da identificação, a senha biológica.

A autenticação biométrica do usuário pode elevar sensivelmente a segurança do sistema e a facilidade de uso, pois o usuário não tem que lembrar seus PINs ou senhas.

Antes do sistema ser utilizado, um processo inicial deve mapear as características biométricas selecionadas. Para isto, a característica é escaneada por sensores especiais, usando um *software* de processamento de imagens ou outra tecnologia para gerar um *template* biométrico; o *template* é armazenado em um meio, ou mídia física, para ser utilizado em um ciclo de comparação.

Quando o acesso da aplicação é requerido, a característica biométrica é novamente escaneada e um *template* é gerado e comparado com o *template*

biométrico armazenado, e a aplicação desbloqueada se o resultado da comparação for positiva.

Leitura Digital (*Fingerprints*) - Benefícios da verificação digital

a) Longa história de uso;
b) Aceito pelo público como um processo seguro;
c) Tecnologicamente avançado;
d) Uma das técnicas mais adequadas

Smart card é um elemento crucial em todo o sistema de segurança que usa assinatura digital e biometria. Não há um caminho mais seguro de armazenamento de chaves secretas e certificados do que um *Smart Card*. O cartão também pode ser usado para encriptar informações e gerar ou verificar assinaturas e certificados.

3.14 QUANTIDADE E DISTRIBUIÇÃO

Estão sendo contemplados nesse projeto todos os militares da ativa, reserva, reformados, dependentes e pensionistas. Essas pessoas serão identificadas no Sistema de Identificação da Aeronáutica e receberão a carteira de identidade do Comando da Aeronáutica. Serão 350.000 (trezentos e cinquenta mil) cartões de identidade que serão distribuídos entre as diversas regiões do País, abrangendo todos os Órgãos do COMAER.

O gráfico da figura 18 mostra a distribuição da quantidade de pessoas, por Comando Aéreo Regional (COMAR) que serão englobadas no projeto. Os dados abaixo foram extraídos do SIGPES em 23/09/2009, e retrata a realidade desse momento. O item vazio corresponde a erros de cadastro existente no Sistema de Informações Gerenciais de Pessoal do Comando da Aeronáutica.

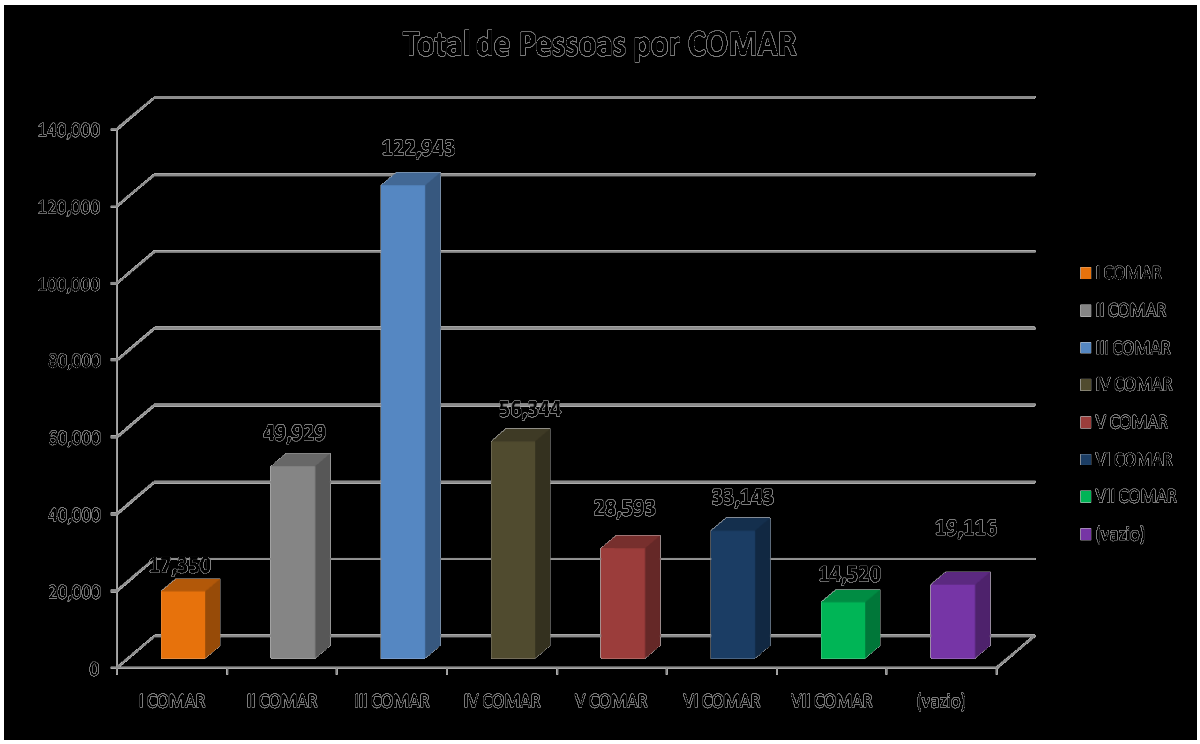


Figura 18: Gráfico de barras (distribuição)
Fonte: Projeto identidade digital do COMAER

3.15 PROJETOS PREVISTOS

A tecnologia que será disponibilizada poderá atender a vários projetos no âmbito do Comando da Aeronáutica, de acordo com a disponibilidade de espaço no cartão, porém, visando definir o escopo pretendido, serão contemplados três projetos na área de pessoal:

a) *Identidade Multifuncional*, que possibilitará o funcionamento dos outros projetos, pela implantação de um cartão de identidade eletrônico multifuncional;

b) O de *Implantação de Controle de Comensais*, que melhorará a qualidade da alimentação fornecida pelo sistema de subsistência, através do aprimoramento do cômputo dos indicadores de desempenho e do replanejamento contínuo baseado nessas informações; e

c) O de *Utilização do cartão multifuncional nas Organizações de Saúde da Aeronáutica* (OSA), visando a utilização do espaço disponível para

aplicações informatizadas na memória embutida do Cartão de Identidade Multifuncional, possibilitando as Organizações de Saúde da Aeronáutica (OSA) tenham condições de utilizá-lo de forma adequada.

A responsabilidade pelo desenvolvimento de cada projeto ficará a cargo das Diretorias subordinadas ao Comando Geral do Pessoal, com as seguintes atribuições:

PROJETO	RESPONSÁVEL
Identidade Multifuncional	[15]DIRAP
Implantação de Controle de Comensais	[16]DIRINT (SDAB)
Utilização do cartão multifuncional nas OSA	[17]DIRSA

Tabela 2: Tabela de projetos e responsáveis
Fonte: Autor

3.16 EFEITOS RESULTANTES DO PROJETO

a) Atualização tecnológica da identidade;
b) Eliminação dos custos de aquisição de crachás despadronizados para diversas soluções;
c) Utilização de um único cartão para todo o pessoal da aeronáutica e para todas as soluções informatizadas internas;
d) Padronização das tecnologias de acesso no âmbito do COMAER;
e) Utilização da certificação digital na mesma cédula da identidade, podendo ser utilizada externamente ao âmbito da Força, após a Autoridade Certificadora do Comando da Aeronáutica estiver emitindo seus certificados, de acordo com o previsto pelo Instituto Nacional de

[15] DIRAP- Diretoria de Administração de Pessoal
[16] DIRINT (SDAB) – Diretoria de Intendência e Subdiretoria de Abastecimento
[17] DIRSA – Diretoria de Saúde

Tecnologia da Informação (ITI);

f) Aumento do número de itens de segurança no cartão de identidade;

g) Legalização da carteira de identidade válida e única, através do RIC, em todo o território nacional;

h) Aumento da eficiência no atendimento hospitalar, devido à possibilidade de acesso rápidos a informações emergenciais;

i) Aumento da segurança no controle ao atendimento de pessoas que fazem direito ao SARAM; e

j) Visualização de indicadores para permitir um melhor planejamento de comensais.

Figura 19: Identidade Digital

Fonte: Projeto de Identidade Digital do COMAER

Com o Projeto de Identidade Multifuncional implementado, o Comando da Aeronáutica possui a oportunidade de se posicionar à vanguarda tecnológica de identificação, disponibilizando a operacionalização da sua Autoridade Certificadora, através das Autoridades Registradoras, atuais SIDOM, além de se destacar, com referência, na redução de custos e simplificação de procedimentos, tendo como consequência da adoção de soluções simples e criativas.

Após identificar a infra estrutura de chaves públicas no COMAER, estabelecida uma comparação entre outros modelos e verificado a importância e os benefícios da utilização da certificação digital, cabe agora destacar os aspectos metodológicos que serão abordados a seguir.

4 METODOLOGIA

Para a realização desta pesquisa científica fez-se necessário definir uma metodologia a fim de disciplinar o trabalho e reunir informações úteis e verossímeis.

Quanto aos meios, este estudo científico utilizou as seguintes técnicas para obtenção de dados:

a) pesquisa bibliográfica: desenvolvida com base em livros, enciclopédias, monografias e artigos científicos, buscas na Internet e na rede interna do Comando da Aeronáutica (Intraer); e
b) pesquisa documental: desenvolvida com base em dispositivos legais; normas e regulamentos da ICP Brasil, disponibilizada pela ITI e pelo Comando da Aeronáutica;
c) Questionário: desenvolvida com base em um questionário em papel aplicado em pessoas selecionadas, por possuir conhecimento especifico;
d) Questionário *on line*: Aplicado ao público em geral pertencente ao Comando da Aeronáutica.

O universo da pesquisa foi composto pelos militares que integram duas áreas na Força, a do sistema de tecnologia da informação do Comando da Aeronáutica e a dos usuários em geral que utilizam a tecnologia da informação para o desempenho de seus afazeres do dia a dia.

Os militares que compõem o sistema de tecnologia da informação do Comando da Aeronáutica, mais especificamente do Centro de Computação da Aeronáutica, foram selecionados e escolhidos por serem especialistas no assunto e trabalharem diretamente na implementação da Certificação Digital na Força.

Estes especialistas foram muito úteis na pesquisa, pois, suas informações contribuíram para identificar o processo utilizado na implementação da certificação no Comando da Aeronáutica e apontaram futuras possibilidades inovadoras ao

sistema bem como a utilização da nova tecnologia em projetos de ponta, já em andamento, que utilizam a tecnologia de chaves.

A esses especialistas, entre eles doutorandos, mestres, pós-graduados e técnicos aplicou-se um questionário que teve como base um formulário em papel composto de 16 perguntas divididas em duas fases. A primeira era constituída da identificação do informante, o que possibilitava verificar sua formação, experiência e conhecimento da Força. A segunda visava coletar informações a respeito do processo de certificação desenvolvido na Força, sua estrutura, seus problemas, o funcionamento, a implementação, os novos projetos e as vantagens, foco principal de nossa pesquisa.

Certamente, essa amostragem não foi suficiente para a generalização das conclusões, desta forma foi utilizado um questionário[18] disponibilizado na rede interna da Força composta de 10 questões que focou um universo mais amplo, o usuário em geral do sistema de tecnologia da informação.

Com a composição dos questionários e pesquisa realizada coletou-se conteúdo suficiente que possibilitou atingir resultados que serviram para justificar a realização da pesquisa com suas devidas conclusões que serão expostas no capitulo final desta dissertação.

Para se ter uma ideia da representatividade da amostragem, o universo de indivíduos do STI (Sistema de Tecnologia da Informação) foi composto por 12 oficiais, entre eles o Comandante do Centro de Computação de Aeronáutica de Brasília, pós graduado na área e mestre pela UNB (Universidade de Brasília), além de chefe do curso de tecnologia da informação da faculdade SENAC de Brasília, o Chefe da Divisão técnica do Centro de Computação, mestre e chefe do curso da faculdade USPI em Brasília e o chefes de subdivisão mestre e professor da Universidade Católica de Brasília, Doutorando e mestre pela UNB com formação no Instituto tecnológico da Aeronáutica e outros militares todos com nível superior e pós graduados *lato sensu*.

[18] Paxonta. Sistema de questionário *on-line* da nova geração. Disponível em: <http://www.paxonta.com>

A segunda fonte de dados foi oriunda de uma pesquisa realizada por meio da internet e direcionada aos usuários em geral da tecnologia de informação, na qual foram expostos 10 questionamentos, os primeiros visando a identificação do usuário, os seguintes visavam obter dados sobre o conhecimento do sistema de chaves públicas, suas usabilidades, confiança e expectativas na melhoria das atividades desenvolvidas na instituição.

Para permitir maior flexibilidade nas respostas, foi utilizada a escala Likert, proposta por Rensis Likert em 1932, onde os respondentes são solicitados não só a concordarem ou discordarem, mas também, a informarem qual o seu grau de concordância/discordância. As proposições foram apresentadas para o grupo, que indica suas reações assinalando as respostas em um dos três grupos: o das respostas afirmativas (concordo plenamente e concordo), o das respostas neutras (não sei/não tenho opinião formada) e o das respostas negativas (discordo e discordo totalmente).

Do ponto de vista de sua natureza este trabalho pode ser considerado uma Pesquisa Básica, de acordo com a definição de Silva e Menezes (2001), pois objetiva extrair da literatura os possíveis tipos de estrutura, padronização e formas de funcionamento de uma infraestrutura de chaves públicas, bem como os benefícios que serão proporcionados por esta infraestrutura ao Comando da Aeronáutica.

Quanto aos objetivos, optou-se pelo caráter exploratório, pois proporciona maior familiaridade com o problema a fim de torná-lo explícito, enquadrando-se na definição de Gil (1991 apud SILVA; MENEZES, 2001).

Por se tratar de um tema que alia tecnologia e formalismo legal, foram apresentados esclarecimentos sobre os seguintes objetivos específicos:

a) Levantar os conceitos de certificação digital no mundo contemporâneo.

Ao alcançar este objetivo, por meio de um extensa pesquisa bibliográfica, foi possível identificar com clareza a definição e o significado da certificação digital como modelo de segurança da informação.

b) analisado os tipos de criptografia;

Por meio de pesquisa documental e bibliográfica foi possível atingir este objetivo, onde foram esclarecidos os tipos de criptografias existentes e o modelo adotado para utilização na certificação digital.

c) Identificar a estrutura reguladora de certificação digital no Brasil?;

Com este passo e por meio de uma pesquisa documental e bibliográfica, apurada, pode-se entender como a teoria da burocratização contribui para estabelecer a infraestrutura de chaves públicas brasileiras bem como conhecer as documentações que normatizam sua estrutura.

d) efetuar uma análise comparativa sobre a utilização da certificação digital em outros países; e

Após este tópico e baseado na pesquisa documental e bibliográfica foi possível se ter uma comparação da estrutura de certificação utilizada no Brasil, seu modelo e a comparação com outros países.

e) verificar a utilização da certificação nas instituições brasileiras e as vantagens que poderão ser agregadas ao COMAER.

Após este tópico e baseado na foi possível se ter uma comparação da estrutura de certificação utilizada no Brasil, seu modelo e a comparação com outros países.

Ao alcançar este objetivo por meio de pesquisa documental, pesquisa bibliográfica e preenchimento de questionários em papel e *on-line* foi possível efetuar uma analogia da utilização da certificação digital nas diversas organizações da esfera federal brasileira com as possíveis utilizações dentro do COMAER.

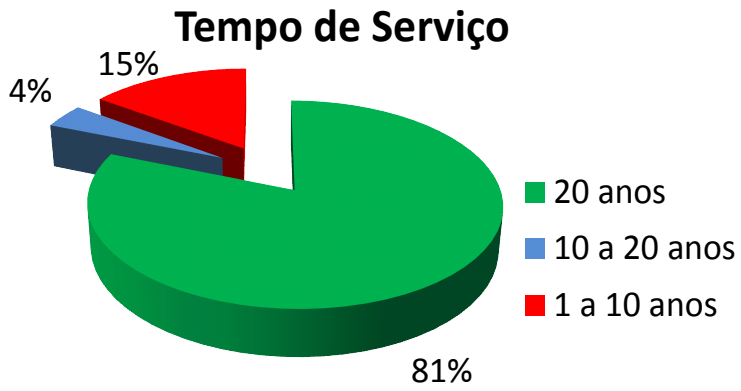
5 ANÁLISE DOS RESULTADOS

Seguindo o que foi descrito na metodologia empregada neste trabalho, conforme especificada no capítulo 4, foram aplicados questionários para dois públicos distintos e com perguntas que visaram ter uma ideia da importância do uso da tecnologia da certificação digital.

5.1 PESQUISA COM USUÁRIOS NÃO ESPECIALIZADOS

A pesquisa *on-line,* realizada com os usuários não especializados deu-se por meio do site Paxonta[19]. Esta pesquisa foi composta por um questionário objetivo com 10 perguntas e respostas diretas, onde a amostra dos resultados obtidos estão apresentados no Anexo A.

Em uma consolidação deste questionário pode-se obter o seguinte resultado.



Fonte: Autor
Figura 20: Gráfico de Idade

Do público entrevistado, 81% são militares, e possuíam 20 anos ou mais de serviço, portanto profissionais que conhecem muito bem as peculiaridades da Força, que somados aos 4% possuidores de mais de 10 anos representam um total de 85% de pessoas que conhecem e entendem os problemas da Força, podendo opinar com clareza e conhecimento apurado.

[19] **Paxonta**. Sistema de questionários on-line da nova geração. Disponível em: <http://www.paxonta.com> direcionado para <http://pt.paxonta.com/index.php?lang=pt&pid=74 >.

Além do demonstrado conhecimento da Força foi possível observar que 85% do entrevistados possuem graduação e pós-graduação, que ainda somado a 4% dos indivíduos possuidores de nível técnico, demonstraram o elevado nível cultural dos entrevistados.

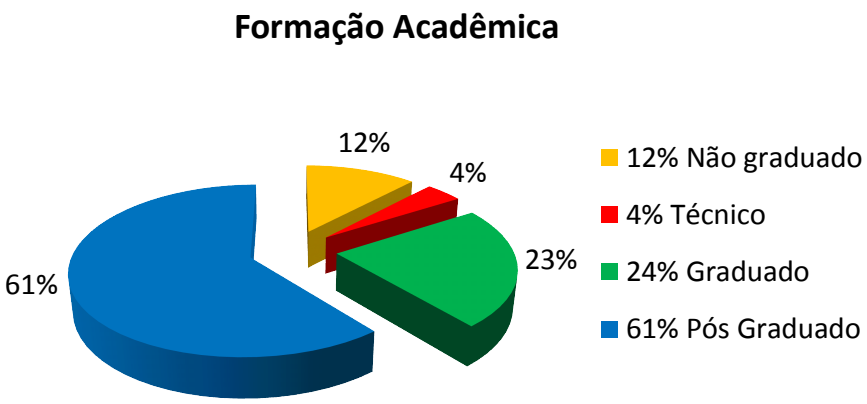


Figura 21: Gráfico de Formação Acadêmica
Fonte: Autor

Observou-se também que 92% dos entrevistados já ouviram falar de algum modo em cerificação digital, e que 96% utilizam senha para acessar o site de seus bancos, retira dinheiro em caixa eletrônico, utilizam cartão de crédito, já acessaram sites seguros ou já digitaram o PIN em seus celulares, demonstrando que já utilizaram de alguma maneira a certificação digital, mesmo sem ter conhecimento do processo que estava por trás do que estavam fazendo ou seja, utilizando a certificação como medida de segurança.

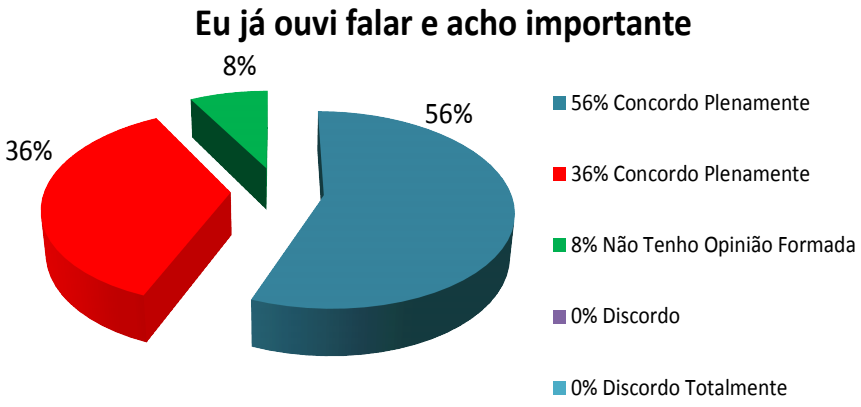


Figura 22: Gráfico de Importância
Fonte: Autor

Constatou-se ainda que 93% dos entrevistados entendem que a certificação digital é algo que traz segurança e otimiza os processos de uma organização.

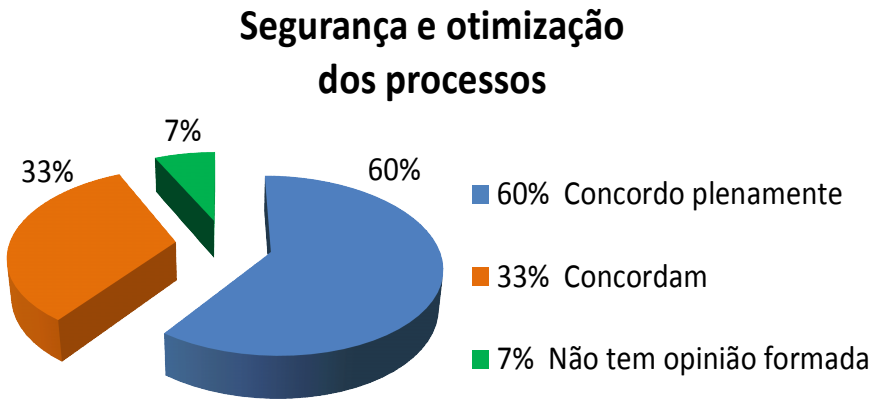


Figura 23: Gráfico de Segurança e Otimização
Fonte: Autor

Um percentual de 93% dos entrevistados usariam com frequência a certificação digital na Força, portanto confiam na segurança que o processo proporciona.

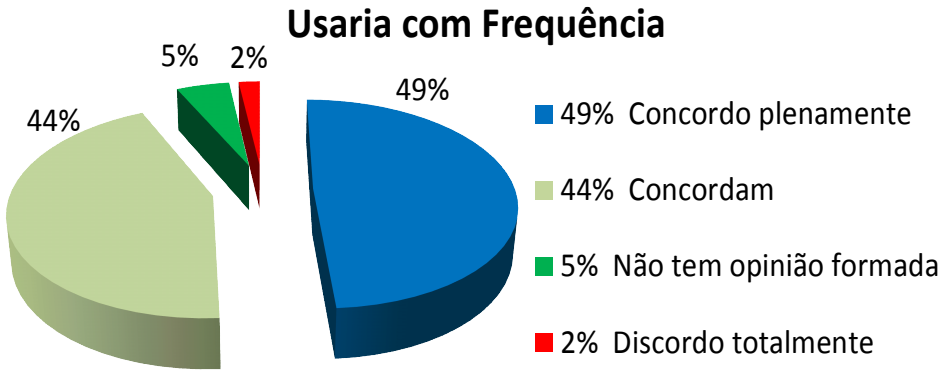


Figura 24: Gráfico de Possibilidade de uso
Fonte: Autor

Em consequência, foi possível constatar que 71% dos entrevistados acreditam que, em breve, os principais sistemas do COMAER estarão utilizando a certificação digital, e que 20% não acreditam ou não possuem opinião formada sobre o assunto e que 9% discordam do assunto.

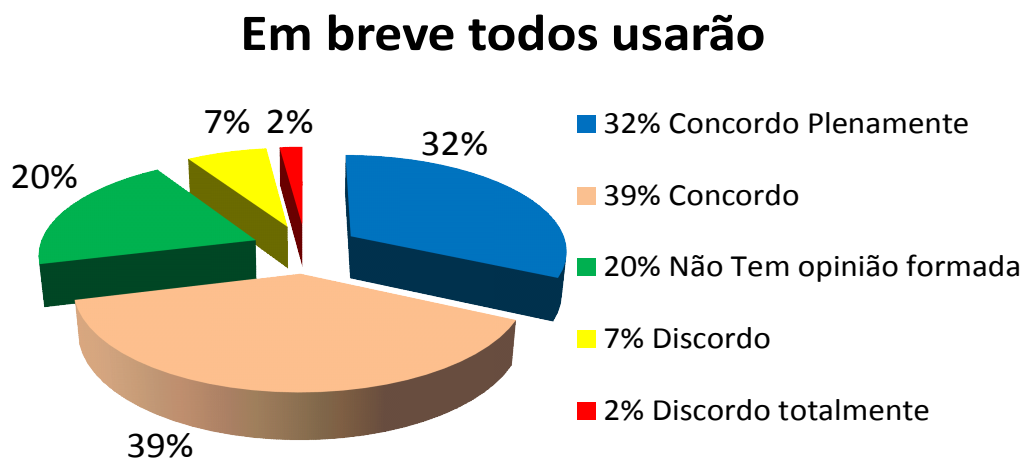


Figura 25: Gráfico utilização
Fonte: Autor

Portanto, nos questionamentos realizados com o público geral, observou-se que o tema é conhecido pela maior parte dos entrevistados e estes julgam que a tecnologia de certificação digital exerce um fator importante no aperfeiçoamento e melhoria dos processos administrativos da organização garantindo a segurança no tráfego de informações.

Torna-se importante observar ainda que este público alvo não é possuidor de conhecimento especializado na área e acredita que a certificação digital em breve estará sendo usada por todos na Força e que se já estivesse disponível estaria usando esta ferramenta com frequência.

5.2 PESQUISA COM USUÁRIOS ESPECIALIZADOS

A pesquisa realizada com os usuários especializados foi composta de um questionário objetivo/subjetivo, e encontra-se neste trabalho como anexo B, porém não pode ser representada em indicadores de forma direta, mas possuem como resultados consolidados a seguinte interpretação:

Como resultados primários dos referidos quesitos observa-se, que no público especializado encontram-se os maiores responsáveis pela implementação da tecnologia de certificação digital no âmbito da Aeronáutica, estes julgaram que a

tecnologia possui uma considerada complexidade para a implementação, mas que o uso cotidiano pelos usuários finais é de fácil manipulação.

Mesmo considerado complexa, a massa crítica de profissionais que conhecem do assunto é suficiente para uma adequada implementação e implantação no contexto da Força no cenário atual.

Observa-se ainda que todos os profissionais entrevistados (especializados e não especializados) consideram que a tecnologia irá prover um melhor desempenho nos trâmites administrativos e operacionais, dentro de um ambiente seguro e eficiente.

Vale ressaltar que as expectativas apresentadas pelos militares especializados serviram como diferenciador respaldada na competência de um gestor (comandante) e na competência técnica de todos entrevistados. Neste caso, a representatividade se confirma por ser o universo de entrevistado constituído de 100% dos responsáveis pela implementação do sistema de certificação digital na Força, possibilitando uma expressiva amostra de conteúdo e de informação.

Constatou-se também que quase a totalidade do profissionais entrevistados (especializados e não especializados) possuem conhecimento organizacional elevado e são possuidores de excelente nível educacional, e que consideram como um assunto de importância, identificando esta ferramenta como algo moderno, que traz segurança e otimiza os processos de uma organização.

Portanto, não existe por parte de todos estes profissionais entrevistados, o receio do novo, do desconhecido, do que será encontrado a frente, e sim a curiosidade e a expectativa com a modernização e melhoria que poderão usufruir desta inovação apresentada.

5.3 ANÁLISE COMPARATIVA ENTRE MODELOS

Observando os modelos anteriormente apresentados no capitulo 3, torne se interessante a realização de uma análise comparativa que levará o leitor uma reflexão sobre o modelo brasileiro.

Quanto aos modelos que se consagraram na Europa e nos Estados Unidos, constata-se que os mesmos trabalham sobre um ambiente de mais de uma

infraestrutura de chaves públicas. Essa estrutura traz um nível maior de complexidade, bem como um nível maior de engenharia política, visando a padronização de regras, normas e determinações.

O modelo americano de infraestrutura de chaves públicas é bastante flexível. A arquitetura *cross over* oferece a possibilidade das Autoridades Certificadoras criarem seus próprios certificados raiz e estabelecerem relações cruzadas com outras entidades, porem sem um domínio concreto do governo americano que ainda tenta estabelecer uma interoperabilidade eficiente entre as empresas privadas que criam seus próprios certificados em cada local do pais.

O algoritmo de criptografia utilizado no modelo americano é uma técnica de domínio público. Isto proporciona certo conforto aos participantes do sistema tendo em vista que todos conhecem a estrutura em que estão confiando e sabem que ele ainda não foi quebrada.

Dessa forma a entidade privada que possuir maior força comercial poderá impor confiança de seu certificado no país e no exterior, como por exemplo a empresa *VeriSign* propulsora da tecnologia naquele país e que possui no Brasil uma filial de nome *CertiSing,* com projeção e confiabilidade na emissão de par chaves (assinatura) nos continentes Europeu, das Américas e no Asiático.

As chaves públicas das Ac´s que operam no mercado americano já estão inseridas no softwares utilizados para navegação como por exemplo o Microsoft Internet Explorer, o Netscape e o Mozila Firefox.

No Brasil, por sua vez, a chave raiz é proveniente do Comitê Gestor da ICP-Brasil e que, para ser reconhecida automaticamente, necessita ser inserida nos softwares de navegação, fato este que ainda não aconteceu, necessitando que cada usuário brasileiro busque manualmente o arquivo e instale-o no seu computador, isto poderá ser um ponto de vulnerabilidade pois será possível que certificados falsos sejam distribuídos pela rede confundindo os usuários menos esclarecidos sobre o assunto. Porem os fabricantes fornecedores destes navegadores já anunciaram que nas próximas versões seus navegadores já possuirão a chave brasileira incluída.

È importante lembrar que de acordo com a comunidade de segurança internacional, ainda não se conhece um método matemático para provar se um algoritmo criptográfico é seguro ou não. O meio utilizado para se testar e descobrir

se um modelo é seguro é publicá-lo em conferencias internacionais de renome, como por exemplo a *Crypto* e *Eurocrypt* ou em conceituados meios de vinculação como o *Bell Systems Techinical Journal*, e assim, ser analisado pelos pesquisadores, especialistas e o público em geral que conheçam métodos sofisticados para quebra de senha. Caso o algoritmo passe por tal avaliação, a industria e a comunidade internacional passa a aceitá-lo como seguro.

Um exemplo deste procedimento foi o caso ocorrido nos Estados Unidos da América, onde uma empresa americana de telefonia, em 1995, desenvolveu um algoritmo criptográfico para o uso na telefonia digital seguro e inquebrável, mantendo, este algoritmo em segredo por 4 anos. Em 1999, exposto o algoritmo desta empresa à comunidade acadêmica internacional, este foi logo quebrado, demonstrando ser frágil e ineficaz para o fim que se destinava.

O Brasil, como relatado anteriormente, ingressou no ramo da certificação digital com um certo atraso fato este, que trouxe vantagens contextuais para o modelo brasileiro, uma vez que, amparados nos problemas dos países precursores e com o apoio do governo federal, criou um novo órgão público denominado ITI, vinculado a casa civil da Presidência da República que, desenhou a arquitetura brasileira, baseada nas teorias da burocratização, departamentalização em uma estrutura *top down* com equipamentos tecnológicos de última geração. Nesse cenário, o país montou sua Infraestrutura de Chaves Públicas, denominada ICP-Brasil.

O modelo brasileiro se beneficiou de uma maior maturidade do sistema de certificação digital. Como o Certificado digital possui uma forte padronização e também um forte componente tecnológico, a inserção tardia propiciou ao Brasil fazer uma opção tendo um cenário de desenvolvimento e pesquisa mais maduro e atualizado no contexto mundial, trazendo com isso uma assertiva maior nas ações de implementação do sistema.

Porém, no modelo brasileiro, o algoritmo de criptografia utiliza tecnologia nacional e foi desenvolvido por um órgão ligado a ABIN (Agência Brasileira de Inteligência). Entretanto, por não ser esse algoritmo de conhecimento público tem-se gerado várias dúvidas sobre a robustez do sistema e sobre a garantia de privacidade.

Atualmente, o governo brasileiro tem migrado os mecanismos de autenticação e proteção dos seus sistemas reguladores, como o SIAFI, SIORG, SIAPE, entre outros, para utilizarem recursos de criptografia baseados em certificados ICP-Brasil, provendo o nível de confiança em transações em meio digital.

Como principal exemplo, temos o sistema de portal de compras do governo, o COMPRASNET, onde licitações na modalidade de pregão eletrônico são realizadas já utilizando certificados digitais como meio de identificação dos pregoeiros e potenciais fornecedores do governo, provendo uma maior transparência e agilidade nos processos governamentais.

Observa-se assim que nenhum dos problemas relatados nos países descritos acima ocorre no brasileiro, onde a certificação digital é única e reconhecida em uma cadeia onde os atores da certificação se estabelecem sobre ela. Essa conformação leva a um modelo racional, onde os investimentos das ações ficaram a cargo do governo brasileiro, determinando uma única estrutura hierárquica sólida e baseada em regras também únicas, padronizando e exercendo o controle central a certificação digital, como pode ser observado no quadro comparativo a seguir.

Quadro comparativo entre modelos

Descrição	Modelo Americano	Modelo brasileiro	Modelo espanhol	Modelo Alemão
Arquitetura	Distribuída	Hierarquizada	Descentralizada	Descentralizada
Criptografia	Algoritmo tornado público	Fruto de uma tecnologia nacional mantida em sigilo pelas autoridades	Algoritmo do estado	Algoritmo do estado e algoritmo privado
Autoridades Certificadoras	Podem operar livremente. È necessária o reconhecimento por outras Acs por meio da certificação cruzada.	Necessitam de certificação do comitê Gestor para poder operar. Posteriormente são fiscalizadas constante.	Existem duas Acs diferentes que operam livremente, apesar de serem do governo necessitam de interoperabilidade certificação cruzada	Somente um grupo de entidades públicas e privadas previamente autorizado pelo governo podem operar livremente
Segurança	A segurança é inerente às Acs. Como elas são independentes, o comprimento de uma não afeta as demais	A chave raiz é um ponto vulnerável do sistema se decifrada coloca em dúvida todo sistema	A segurança é inerente a cada AC. Operam independentes, o comprimento de uma não afeta a outra.	A segurança é inerente a cada AC.
Privacidade	Teoricamente o serviço de inteligência do governo não tem como espionar as pessoas. Porem a necessidade de interoperabilidade torna o sistema confuso e sujeito a fraudes.	Sendo o governo detentor da chave raiz que por sua vez usa algoritmo de criptografia nacional e sigilos, vislumbra-se a possibilidade de intervenção do governo por meio de espionagem sem o conhecimento do autor.	Sendo o governo detentor das chaves raiz vislumbra-se a possibilidade de intervenção do governo por meio de espionagem sem o conhecimento do autor.	Ponto forte do sistema alemão, pois entidades privadas possuem autorização de emissão de chaves. Teoricamente o governo não tem como espionar as pessoas, pois cada entidade autorizada possui sua chave.
Navegadores	As principais Acs já possuem suas chaves raiz registradas e disponibilizadas nos navegadores em uso.	A chave raiz virá inserida nos próximos navegadores entretanto enquanto isto não acontece existe a possibilidade de chaves falsas	As principais Acs já possuem suas chaves raiz registradas e disponibilizadas nos navegadores	As principais Acs já possuem suas chaves raiz registradas e disponibilizadas nos navegadores

Tabela 1: Quadro comparativo entre modelos.
Fonte: Autor.

Portanto, por meio desta análise comparativa, e neste cenário, observou-se que, mesmo sendo estes países de primeiro mundo e precursores desta área do conhecimento, não obtiveram a liderança na área, nem mesmo o direito de possuírem a melhor estrutura de certificação digital no mundo.

Por outro lado, o Brasil por ingressar na atividade de estrutura digital tardiamente, trouxe a possibilidade de apreciar os erros e acertos de outros e repensar sua estrutura e seu projeto proporcionando subsídios para a escolha do melhor modelo bem como a melhor forma de implementá-lo com sucesso.

Desta forma, a certificação brasileira tornou-se, em pouco tempo, um exemplo a ser seguido por outros países, o que já vem acontecendo, como pode ser notado, em países da América do Sul como Argentina e Uruguai, que estão trabalhando para criação de um modelo baseado no do Brasil.

6 CONCLUSÃO

Este trabalho teve como objetivo geral apresentar os benefícios provenientes da certificação digital que poderão otimizar os serviços da administração interna do COMAER.

O presente estudo conclui que a certificação digital no Brasil acompanha o que há de mais moderno no conceito mundial, e em breve, proporcionará aos diversos setores da sociedade uma mudança cultural, administrativa e operacional ao imprimir agilidade, segurança, integridade e autenticidade ao trâmite de todas informações institucionais disponibilizadas eletronicamente, e deverá estar fortemente enraizada na vida das organizações do COMAER nos próximos anos, fazendo parte do dia a dia de todos os militares.

Por meio de uma extensa pesquisa bibliográfica foi possível esclarecer o significado da certificação digital, estabelecer sua importância e traçar um paralelo entre o modelo Brasileiro e os aplicados em outros países do mundo.

O foco deste trabalho foi direcionado para uma análise dos conceitos da certificação no país, sua estrutura de normatização e seu significado, em paralelo aos benefícios possíveis oriundos da conclusão do projeto de certificação digital do Comando da Aeronáutica.

No início, apresentou-se a importância que o assunto vêm recebendo no contexto internacional, relevância com o qual é tratado pelo no governo brasileiro e seu reconhecimento no âmbito militar. Foi constatado principalmente que o modelo Brasileiro passa a ser uma referência mundial, por se tratar de uma estrutura bem elaborada e com respaldo jurídico reconhecido pelas instituições governamentais.

Na sequência, esclareceu-se o que vem a ser a tão falada certificação digital, seus critérios de integridade, autenticidade, sigilo e irrefutabilidade.

Foram comentados, também, aspectos da criptografia e os tipos de algorítimos criptográficos mais usados, além do mecanismo utilizado para a assinatura digital. Foi concluído que a implementação e a regulamentação do uso do certificado digital envolvem operações complexas, mas que o uso é extremamente simples na essência da operação dos sistemas computacionais.

Por conseguinte, abordou-se a estrutura reguladora da certificação digital, seus componentes, o modelo, as obrigações e a estrutura, à luz da medida Provisória n° 2200-2, que institui a infraestrutura de chaves públicas brasileira bem como as normas e legislações do Instituto Nacional de Tecnologia da Informação. Observou-se que o órgão normatizador no Brasil (ITI) tem um papel fundamental na elaboração de resoluções, homologações e validação nos demais órgãos que compõem a infraestrutura de chaves públicas Brasileira.

Vários aspectos e problemas inerentes à certificação digital foram abordados, utilizando uma visão bastante atual dos conceitos nos cenários nacionais e internacionais da certificação, resultando em uma comparação dos modelos empregados nos países desenvolvidos do continente americano e europeu.

Desta forma, foi possível concluir que o modelo empregado no Brasil encontra-se no nível mundial de excelência, merecendo destaque e colocando o Brasil, mais uma vez, como referência quanto ao modelo escolhido, no uso e na empregabilidade da certificação digital. Este destaque deve-se ao fato do Governo Brasileiro ter adotado um modelo baseado na teoria da burocratização, distribuída em uma estrutura hierarquizada e centralizada, em forma de árvore, facilitando o rígido controle e normatização por parte do governo federal, em um processo único.

Foram abordados, no decorrer do trabalho, aspectos relacionados a vertentes do setor produtivo, notadamente a economia digital, bem como aspectos diretamente relacionados à tecnologia e ao modelo regulatório tratados de forma adequada ao entendimento do leitor. A economia digital, uma das maiores vertentes da nova economia, foi enfatizada no conteúdo desta pesquisa pois é o maior precursor da tecnologia da certificação digital no país e no mundo. O trabalho abordou, também, as diversas possibilidades de aplicação da assinatura digital, dentro e fora do Comando da Aeronáutica. Concluiu-se que o uso da certificação digital no âmbito da Aeronáutica trará inúmeros benefícios, os quais foram enumerados no decorrer do trabalho.

No Comando da Aeronáutica, particularmente, a certificação digital proporcionará aos diversos setores da administração características de segurança, integridade, autenticidade e irretratabilidade como pilares de uma nova era no trâmite de informação. A maior garantia de segurança que caracterizava essa

ferramenta garantirá o tráfego de informações classificadas e sigilosas, além de imputar um maior grau de confiabilidade no intercâmbio de informações.

Na área operacional, a certificação digital permitirá o trâmite de mensagens e documentos com segurança e integridade, proporcionando aos Exercícios e Manobras as vantagens da criptografia e autenticação dos dados.

Um desses conceitos, largamente difundido nas atividades militares operacionais, é conhecido como C3I (comando, controle, comunicações e inteligência) que possui como objetivo o da melhor exploração do emprego da força com equidade e eficiência. Na prática, um sistema C3I consiste de pessoas, organizações e doutrina, interagindo com sistemas físicos, tais como plataformas, sensores, telecomunicadores, processadores de imagens e meios de ação, num ambiente incerto, procurando assegurar com que ações defensivas e ofensivas, sejam executadas de modo mais rápido e seguro com os possíveis danos dimensionados para cada ação especifica.

Portanto, é de se observar que os diversos serviços prestados pela Internet, alguns deles já comentados durante o presente trabalho também poderão ser adaptados ao efetivo da Aeronáutica, utilizando a certificação digital como instrumento de suporte seguro para o Comando da Aeronáutica e seu público interno.

Todos os aspectos relatados no presente trabalho, cujas características apontam para a excelência da certificação digital no Brasil e, particularmente no Comando da Aeronáutica, viabilizam sua utilização para a melhoria dos serviços da administração interna no COMAER.

Como perspectivas futuras, torna-se importante ressaltar que a tecnologia relacionada à certificação digital e o seu uso no âmbito da Aeronáutica é uma tarefa que merece ser destacada e divulgada pelos profissionais da área, uma vez que a massa crítica hoje existente plantou a semente que está crescendo e estará melhorando cada vez mais a Instituição em seu carater administrativos e operacionais.

REFERÊNCIAS

ASSOCIAÇAO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**: tecnologia da informação código de prática para a gestão da segurança da informação. Rio de Janeiro, 2002.

ADAMN, C.; LLOYD, S. **Understanding PKI** – Concepts, standards, and deplyment considerations: EUA: Addison-Wesley, 2003.

BEAL, Adriana. **Segurança da informação:** princípios e melhores práticas para proteção de ativos de informação nas organizações. Rio de Janeiro: Atlas, 2001.

BRASIL. Centro de Computação da Aeronáutica de Brasília. **Parecer Técnico.** Brasília, DF, 2008a. 3 p.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. **Diretrizes Específicas para os Centros de Computação da Aeronáutica (CCA):** NSCA 7-6. Brasília, DF, 2005.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. **NSCA 7-13:** segurança de sistemas de tecnologia da informação no comando da aeronáutica. Rio de Janeiro, 2006a.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. **DCA 14-8**: política de segurança da informação no comando da aeronáutica. Brasília, DF, 2006b.

BRASIL. Comando da Aeronáutica. **Política do Comando da Aeronáutica para a Tecnologia da Informação: DCA 14-7**. Brasília, DF, 2004.

BRASIL. Ministério da Aeronáutica. Estado-Maior da Aeronáutica. **DMA 7-1**: política de informática do ministério da aeronáutica. Brasília, DF, 1993b.

BRASIL. Presidência da República. Casa Civil. **Decreto nº 3.996, de 31 de outubro de 2001.** Dispõe sobre a prestação de serviços de certificação digital no âmbito da administração pública federal. **Diário Oficial [da] República Federativa do Brasil,** Brasília, DF, 2001b. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/Decretos/DECRETO_3_996_DE_31_10_2001.PDF>. Acesso em: 16 mar. 2008.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui a política de segurança da informação nos órgãos e entidades da administração pública federal. **Diário Oficial [da] República Federativa do Brasil,** Brasília, DF, 2000.

BRASIL. Instituto Nacional de Tecnologia da Informação. **Resolução nº 39, do Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira, de 18 de abril de 2006a.** Aprova a versão 2.0 da Política de Segurança da Informação da ICPBrasil. Disponível em:

<http://www.iti.gov.br/twiki/pub/Certificacao/Resolucoes/RESOLU__O_39_DE_18_04_2006.PDF>. Acesso em: 18 junho 2008.

BRASIL. Presidência da República. Subchefia para Assuntos Jurídicos. **Decreto nº 3.587, de 5 de setembro de 2000**. Estabelece normas para criação da Infra-Estrutura de Chaves Públicas do Poder Executivo Federal – ICP-Gov, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3587.htm>. Acesso em: 16 fev. 2010.

BRASIL. Universidade da Força Aérea. Escola de Comando e Estado-Maior da Aeronáutica. **Instruções iniciais para elaboração da monografia do Curso de Comando e Estado Maior 2008b**. Disponível em: <http://www.ecemar.intraer/monog2008.htm>. Acesso em: 18 jun. 2008.

BROERING, Evandro. **Problemas dos projetos atuais**. Disponível em: <http://www.portaljava.com.br/home/modules.php?name=News&file=article&sid=425>. Acesso em: 30 mar. 2008.

CÂMARA Brasileira de comércio eletrônico. **Cartilha digital**. Disponível em: <http://www.ibpbrasil.com.br/certificacaodigital/images/guia.pdf>. Acesso em: 18 maio 2008.

CHIAVENATO, Idalberto. **Teoria geral da administração**. Rio de Janeiro: Campus, 2001. 1v.

CERTISIGN, Empresa de certificação digital. **Peticionamento eletrônico** Disponível em: <http://www.certisign.com.br>. Acesso em: 12 abr. 2008.

_____ Decreto nº 3.872, de 18 de julho de 2001. Dispõe sobre o comitê gestor da infra-estrutura de chaves públicas brasileira – ICP-Brasil. **Diário Oficial [da] República Federativa do Brasil, Brasília,** DF, 2001a.

EMBAIXADA DA ALEMANHA. **Infra estrutura de chaves públicas alemã.** Brasília, DF, 2004. 18 dispositivos, color.

EMBAIXADA DA ESPANHA. **Infra estrutura de chaves públicas da espanha.** Brasília, DF, 2004. 23 dispositivos, colorido.

Federal Bridge Certification Authority. Disponível em: <http://www.fbca.org.uk>. Acesso em: 23 maio 2008.

FEGHHIN, J.; WILLIANM P. **Digital certificates, appliend Internet security**. EUA: Addison-Wesley, 2000.

GAIMP. **Grupo de Acompanhamento da Informatização do Ministério Público.** Disponível em: <http://www.mp.sp.gov.br/portal/page/portal/gaimp/manuais/glossario.htm>. Acesso em: 26 mar. 2008.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2007.

GOMES, Maria Paulina. **Construindo soluções acadêmicas**: monografias, dissertações e teses do projeto a defesa. Rio de Janeiro: UNIFA, 2007.

_____ **Introdução à teoria geral da administração**: uma visão abrangente da moderna administração das organizações. Rio de Janeiro: Campus, 2003.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **ICP BRASIL.** Disponível em: <http://acraiz.icpbrasil.gov.br>. Acesso em: 12 abr. 2008.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de Metodologia Científica**. 6. ed. São Paulo: Atlas, 2007.

Lei de Assinatura Digital. Disponível em: <http://www.iid.de/rahmen/iukdge.html>. Acesso em: 20 maio 2008.

Legislação ICP BRASIL. Disponível em:<http://www.icpbrasil.gov.br>. Acesso em: 12 abr. 2008.

LENOTTI, José Roberto. Infraestrutura de Chaves Públicas, um estudo comparativo entre o modelo brasileiro e o modelo americano. São paulo: Faculdade de Ciências da Unesp, 2002

LIMA, Claudionei Quaresma. **Rotas Hierarquicas e Seguras em Redes Ad Hoc**, 2006. 145 f. Dissertação (Mestrado) Curso de pós-graduação em eletrônica e computação, Instituto Tecnológico da Aeronáutica, São José dos Campos, SP, 2006.

MAJDENBAUM, Azriel; LOPES, Leandro. **Uma proposta para processo de requisitos de desenvolvimento distribuído de software**. Disponível em: <http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER03/leandro_majdenbaum.pdf>. Acesso em: 10 mar. 2008.

MARTINS, João Pedro. **Rede de Computadores**: fatores de vulnerabilidades físicas. 2005. Monografia – Escola de Comando e Estado-Maior da Aeronáutica, Universidade da Força Aérea, Rio de Janeiro, 2005. 13 p.

_____ Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil, Brasília,** DF, 2001c.

MORENO, Edward David; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em Software e Hardware**. São Paulo: Novatec, 2005.

Paxonta. Sistema de questionários on-line da nova geração. Disponível em: <http://www.paxonta.com> direcionado para <http://pt.paxonta.com/index.php?lang=pt&pid=74 >. Acesso em 15 nov. 2010.

PECK, Patricia. **Direito digital**. São Paulo: Saraiva, 2002.

_____ **Resolução nº 41, do Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira, de 18 de abril de 2006b**. Aprova a versão 2.0 dos Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/Resolucoes/RESOLU__O_41_DE_18_04_2006.PDF>. Acesso em: 23 maio 2008.

_____ **Resolução nº 42, do Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira, de 18 de abril de 2006c**. Aprova a versão 2.0 dos Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/Resolucoes/RESOLU__O_42_DE_18_04_2006.PDF>. Acesso em: 18 mar. 2008.

_____ **Resolução nº 47, do Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira, de 03 de dezembro de 2007**. Aprova a versão 3.0 dos Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICPBrasil. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/Resolucoes/Resolucao_47.pdf>. Acesso em: 19 maio 2008.

SANTOS, Luiz Carlos. **Como funciona a criptografia?** Disponível em: <http://www.malima.com.br/article_read.asp?id=65>. Acesso em: 11 jul. 2008.

SANTOS, Neide. **Internet e Web**. Notas de aula. 2000. Disponível em: <http://www.ime.uerj.br/~neide/Internet.htm>. Acesso em: 26 mar. 2008.

SCARTEZINI, V. **Governo e comércio eletrônico nos países em desenvolvimento**. In: FERRER, F.; SANTOS, P. (Orgs). *E-government: o governo eletrônico no Brasil*. São Paulo: Saraiva, 2004. p 3-15.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**. 9. ed. Rio de Janeiro: Elsevier, 2003.

SILVA, Lino Sarlo da. **Public Key Infrastructure PKI**. 1 ed. São Paulo: Novatec, 2004.

SIPSER, Michael. **Introdução à Teoria da Computação**. 2. ed. São Paulo: Thomson, 2007.

Smart Card. Disponível em: <http://pt.wikipedia.org/wiki/Smart_card>. Acesso em: 25 setembro 2009.

STALLINGS, W. **Cryptography and network security principles and practice.** 3 nd. ed. EUA: Prentice Hall, 2002.

TERADA, Routo. **Segurança de dados:** criptografia em redes de computador. São Paulo: Edgard Blücher, 2000.

TEIXEIRA Filho, J. **Gerenciamento conhecimento**: como a empresa pode usar a memória organizacional e a inteligência competitiva no desenvolvimento de negócios. 2 ed. Rio de Janeiro: SENAC, 2001.

TIPTON, H.; KRAUSE, M. **Information security management handbook.** 4 th ed. EUA: Auerbach, 2001.

TKOTZ,V. **Criptografia: segredos embalados para viagem**. São Paulo: Novatec, 2005.

VILHENA, R. **Governo eletrônico: transparência e interface com o cidadão**. In: *Balanço da reforma do estado no Brasil: a nova gestão pública*. Brasília: Ministério do Planejamento, orçamento e Gestão, 2002. p. 115-122.

VOLPI, Marlon Marcelo. **Assinatura Digital**: aspectos técnicos, práticos e legais. Rio de Janeiro: Axcel Books, 2001.

WIKIPEDIA. Enciclopédia Livre. 2008. Disponível em: <http://pt.wikipedia.org>. Acesso em: 10 agosto 2008.

ZUGMAN,F. **Governo eletrônico: saiba tudo sobre essa revolução**. São Paulo: Livro Pronto, 2006.

GLOSSÁRIO

Ameaça - Toda e qualquer condição adversa capaz de vir a causar alguma perda para a empresa. Ameaça é uma condição latente e potencial. Ela não irá causar necessariamente um dano.

Autenticidade - garantia de que o dado ou informação é verdadeiro e fidedigno, tanto na origem, quanto no destino;

Autenticação - A autenticação é um processo que busca verificar a identidade digital do usuário de um sistema, normalmente, no momento em que ele requisita um *log in* (acesso) em um programa ou computador. A autenticação normalmente depende de um ou mais "fatores de autenticação";

CAB – organização militar da aeronáutica responsável pelas aquisições da força no exterior bem como representação da mesma na fms denominada comissão aeronáutica brasileira;

Cartão de tarja magnética - É um objeto de plástico de formato retângular em que pode armazenar qualquer tipo de dados digitais, através de uma tarja preta (magnético), que se localiza no verso do cartão;

CDS – organização militar do exército brasileiro responsável pelos projetos computacionais da força denominado centro de desenvolvimento de sistemas do exército;

Certificação Digital - Os computadores e a Internet são largamente utilizados para o processamento de dados e para a troca de mensagens e documentos entre cidadãos, governo e empresas. No entanto, estas transações eletrônicas necessitam da adoção de mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade às informações eletrônicas. A certificação digital é a tecnologia que provê estes mecanismos.É a tecnologia responsável por prover os mecanismos necessários que visam garantir a autenticidade, confidencialidade e integridade das informações;

Confiabilidade - garantir que, mesmo em condições adversas, o sistema atuará conforme esperado;

CO-PROCESSADOR DO CHIP - É uma Unidade Central de Processamento, UCP, de computador usada para suplementar as funções do microprocessador principal;

CLOCK - Clock é o sinal de temporização usado em uma transmissão on-line. Genericamente uma fonte de sinal de temporização para seqüenciamento de eventos.

Clonagem - É uma cópia da tarja magnética de um ***cartão*** legítimo e aplicada num ***cartão*** falso;

Criptografia - É o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado;

CHIP - O Chip é um dispositivo eletrônico o qual possui milhões de circuitos integrados (ou até em alguns casos microprocessadores). São utilizados para consoles de videogames, computadores, telefones celulares e eletrodomésticos, etc.

Desastre - É o impacto de uma força externa, agressiva, ocasionando perda ou prejuízo significativo. Trata-se de qualquer evento que gere inabilidade em toda ou parte da organização, em suas atividades de negócios, sem predeterminação de tempo. Um desastre não precisa ser necessariamente destruidor. Em alguns casos ele é apenas uma condição que impede a operação de uma atividade crítica, necessária para a geração de um serviço ou produto. Termos semelhantes: interrupção empresarial, catástrofe, tragédia.

Disponibilidade - Garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores e a área de informática;

e-business – conjunto de transações eletrônicas realizadas via rede de computadores. dá-se o nome de e-business aos negócios virtuais feitos por meio de mídia eletrônica.

Finger Print - É um dispositivo cujo propósito é a substituição de senhas pelo uso da impressão digital;

Handheld - Computador de mão, também conhecido como PDA, Pocket PC ou Palm top. Equipamento portátil desenvolvido para servir como dispositivo de acesso, apesar de alguns modelos possuírem uma grande capacidade de memória e de processamento.

Hackers - Pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinada ambiente para proveito próprio ou de terceiros. Dependendo dos objetivos da ação, podem ser chamados de Cracker, Lammer ou BlackHat.

I/O - É uma sigla para Input/Output, em português E/S ou Entrada/Saída. Este termo é utilizado quase que exclusivamente no ramo da computação (ou informática), indicando entrada (inserção) de dados por meio de algum código ou programa, para algum outro programa ou hardware, bem como a sua saída (obtenção de dados) ou retorno de dados, como resultado de alguma operação de algum programa, conseqüentemente resultado de algum input;

Infra-estrutura de chaves públicas – Conjunto de atividades e ações estabelecidas em um processo determinado, visando atender o sistema de criptografia baseado em chaves assimétricas;

Internet – uma internet é uma rede de mundial de computadores que assenta sobre a suite de protocolos tcp/ip;

Intranet – uma intranet é uma rede de computadores privada que assenta sobre a suite de protocolos da internet. conseqüentemente, todos os conceitos da última aplicam-se também numa intranet como, por exemplo, o paradigma de cliente-servidor. Resumidamente, o conceito de intranet pode ser interpretado como "uma versão privada da internet", ou uma mini-internet confinada a uma organização.o termo foi utilizado pela primeira vez a 19 de abril de 1995, num artigo da autoria técnica de stephen lawton[1], na digital news & reviews.

Integridade - garantia de que as informações e métodos de processamento somente sejam alterados mediante ações planejadas e autorizadas;

Irrefutabilidade – O que não se pode refutar, evidente, claro;

LAN (Local Area Network) - Rede de computadores de área local.

Linux - Sistema operacional de arquitetura aberta, utilizado em servidores CISC.

Logs - registros das modificações realizadas nos arquivos de dados;

MICROCONTROLADOR RISC - É um circuito integrado de alta performance que possui internamente um microprocessador e todos os periféricos essenciais ao seu funcionamento como: memória de programa; memória de dados; dispositivo de seleção de entrada e saída; temporizadores e contadores; clock; e dispositivo controlador de interrupção.

RFID - Trata-se de um método de identificação automática através de sinais de rádio, recuperando e armazenando dados remotamente através de dispositivos chamados de *tags* RFID;

Roteadores - é um equipamento usado para fazer a comutação de protocolos, a comunicação entre diferentes redes de computadores provendo a comunicação entre computadores distantes entre si;

ROM - Espaço da memória que contém informações fundamentais para a inicialização do computador, garantindo, por exemplo, o acionamento dos drives de CD-ROM, disco rígido ou flexível e a chamada do sistema operacional.

Servidor - Computador configurado para fornecer serviços. (MARTINS, 2005, p. 48).

Sigilo – O que não se divulga, segredo, reservado;

SIGN PAD - Equipamento eletrônico capaz de escanear a assinatura e reproduzí-la digitalizada;

Smart Card - É um cartão que geralmente assemelha-se em forma e tamanho a um cartão de crédito convencional de plástico com tarja magnética. Além de ser usado em cartões bancários e de identificação pessoal, é encontrado também nos

celulares GSM (o "chip" localizado normalmente atrás da bateria). A grande diferença é que ele possui capacidade de processamento pois embute um microprocessador e memória (que armazena vários tipos de informação na forma eletrônica), ambos com sofisticados mecanismos de segurança.

Tecnologia da Informação - Solução ou conjunto de soluções sistematizadas, baseada no uso de métodos, recursos de informática, de comunicação e de multimídia que visam resolver problemas relativos à geração, tratamento, processamento, armazenamento, veiculação e reprodução de dados, e a subsidiar processos que convertem dados em informação. (BEAL, 2005, *apud* MARTINS, 2005, p. 48);

Template - São designs pré-definidos de apresentação de um Blog. Podem ter imagens ou não, e diferem no tipo de estrutura (duas colunas, três colunas, etc) a distribuição dos vários campos varia de um Template para o outro, e são ampla e facilmente personalizáveis;

Token - É um dispositivo eletrônico, geralmente ligado a porta USB do computador, que gera uma nova senha numérica aleatória a cada 36 segundos ou segundo a programação previamente realizada, para ser utilizada como um fator de segurança adicional em transações financeiras realizadas pela Internet. Este sistema garante total privacidade em caso de roubo de senhas, através de programas espiões como os trojans;

Vulnerabilidade - Ponto onde qualquer sistema é suscetível a um ataque, ou seja, condição encontrada em determinados recursos, processos, configurações, etc., causada, muitas vezes, pela ausência ou ineficiência das medidas de proteção utilizadas com o intuito de salvaguardar os bens da empresa. (MARTINS, 2005, p. 48).

WAN (*WIDE AREA NETWORK*) - Como uma LAN, só que com alcance territorial, regional, nacional e até intercontinental, sendo até mesmo possível em cidades ou continentes diferentes. Empresas públicas como as companhias de telefone fazem parte das WANs; aquelas muito grandes podem ter seu próprio satélite estacionário ou torres de microondas. (MÓDULO, 2004, p. 17).

Wegand - Trata-se de uma tecnologia relacionada ao uso de cartões e leitoras que, além de serem mais duráveis e baratos, oferecem alto nível de segurança.

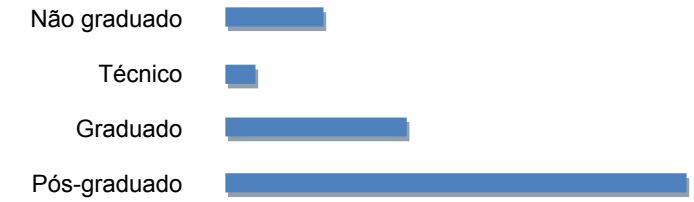
ANEXO A

QUESTIONÁRIO

1. Há quanto tempo está na Aeronáutica?

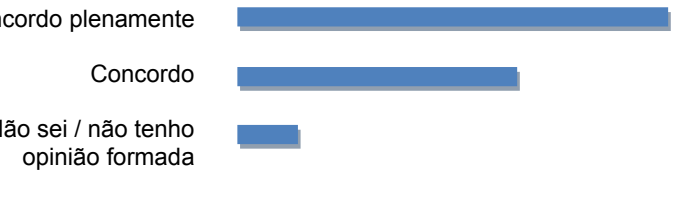
	Percentagem	Respostas
De 1 a 10 anos	14%	8
De 10 a 20 anos	4%	2
Mais de 20 anos	82%	46
Todas as respostas		56
Ignorado		0

2. Qual a sua formação acadêmica / profissional



	Percentagem	Respostas
Não graduado	12%	7
Técnico	4%	2
Graduado	23%	13
Pós-graduado	61%	34
Todas as respostas		56
Ignorado		0

3. Eu já ouvi falar em certificação digital e acho importante!

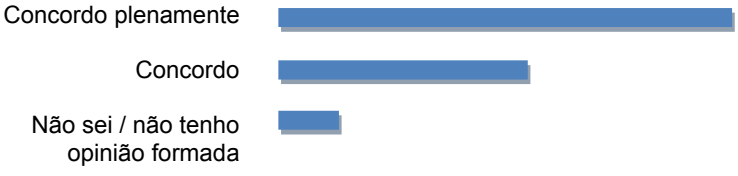


	Percentagem	Respostas
Concordo plenamente	56%	31
Concordo	36%	20
Não sei / não tenho opinião formada	8%	4
Discordo	0%	0
Discordo totalmente	0%	0
Todas as respostas		56
Ignorado		0

4. Eu utilizo senha para acessar o site de meu banco, ou retiro dinheiro em caixa eletrônico, ou utilizo cartão de crédito, ou já acessei sites seguros ou já digitei o nº PIN em meu celular!

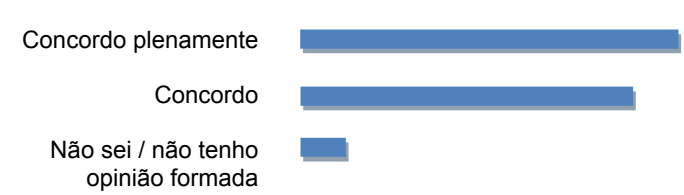
	Percentagem	Respostas
Concordo plenamente	53%	30
Concordo	43%	24
Não sei / não tenho opinião formada	2%	1
Discordo	2%	1
Discordo totalmente	0%	0
Todas as respostas		56
Ignorado		0

5. A certificação digital é algo que traz segurança e otimiza os processos em uma organização!



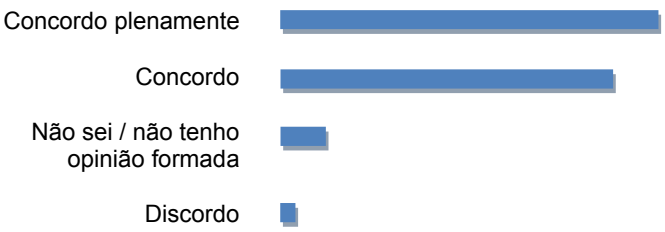
	Percentagem	Respostas
Concordo plenamente	60%	33
Concordo	33%	18
Não sei / não tenho opinião formada	7%	4
Discordo	0%	0
Discordo totalmente	0%	0
Todas as respostas		55
Ignorado		1

6. A Certificação Digital é uma ferramenta moderna, segura e importante para melhoria da gestão organizacional?



	Percentagem	Respostas
Concordo plenamente	49%	27
Concordo	44%	24
Não sei / não tenho opinião formada	5%	3
Discordo	2%	1
Discordo totalmente	0%	0
Todas as respostas		55
Ignorado		1

7. Se eu tivesse uma assinatura digital usaria com freqüência!

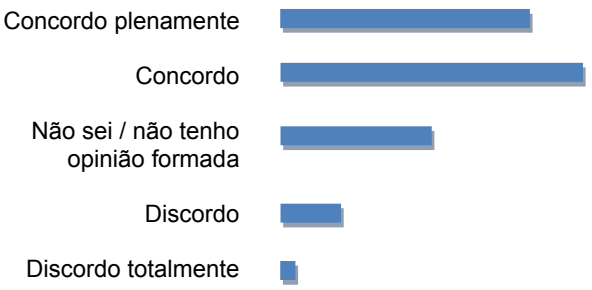


	Percentagem	Respostas
Concordo plenamente	49%	27
Concordo	44%	24
Não sei / não tenho opinião formada	5%	3
Discordo	2%	1
Discordo totalmente	0%	0
Todas as respostas		55
Ignorado		1

8. A certificação digital será mais um desses projetos que não dará em nada!

	Percentagem	Respostas
Concordo plenamente	0%	0
Concordo	0%	0
Não sei / não tenho opinião formada	11%	6
Discordo	59%	33
Discordo totalmente	30%	17
Todas as respostas		56
Ignorado		0

9. Em Breve os principais sistemas do COMAER utilizarão assinatura digital!



	Percentagem	Respostas
Concordo plenamente	32%	18
Concordo	39%	22
Não sei / não tenho opinião formada	20%	11
Discordo	7%	4
Discordo totalmente	2%	1
Todas as respostas		56
Ignorado		0

10. Eu já utilizei e utilizo a certificação digital no meu dia a dia!

	Percentagem	Respostas
Concordo plenamente	14%	8
Concordo	51%	30
Não sei / não tenho opinião formada	3%	2
Discordo	21%	12
Discordo totalmente	11%	6
Todas as respostas		56
Ignorado		0

UNIVERSIDADE DA FORÇA AÉREA

DIVISÃO DE ENSINO

QUESTIONÁRIO

Este instrumento tem por objetivo obter dados com vistas a fornecer subsídios para uma dissertação. Suas respostas são fundamentais para qualificar as informações geradas a partir deste instrumento.

1ª Parte – IDENTIFICAÇÃO DO INFORMANTE

Nome:

Para as questões de múltipla escolha, preencha com X.

1) Sexo: ( ) Masculino ( ) Feminino

2) Idade:
( ) de 21 a 30 anos
( ) de 31 a 40 anos
( ) de 41 a 50 anos
( ) mais de 50 anos

3) Há quanto tempo está na Aeronáutica?
( ) de 1 a 10 anos
( ) de 10 a 15 anos
( ) de 15 a 20 anos
( ) mais de 20 anos

4) Qual sua formação acadêmica/profissional?

( ) Não graduado

( ) Técnico. Em que?_____.

( ) Graduado. Qual curso?_____.

( ) Pós-graduado. Qual curso?_____.

( ) Outros. Qual?_____.

2ª Parte – CERTIFICADO DIGITAL

Para as questões de múltipla escolha, preencha com X.

5) O Senhor(a) conhece certificação digital?

( ) Sim

( ) Não

6) O senhor(a) já utilizou certificação digital?

( ) Sim

( ) Não

Onde?_____
_____

7) O Senhor(a) conhece certificação digital de outros países? Caso afirmativo, cite quais:

( ) Sim. Quais Países?_____

( ) Não

6) O Senhor(a) acredita que o uso da certificação digital é algo que otimiza os processos em uma organização?

( ) Sim

( ) Não

Comente sua resposta: _____
_____
_____

7) No seu local de trabalho o Senhor(a) utiliza ou já utilizou assinatura digital?

( ) Sim.

( ) Não. Por quê? _____

8) O Senhor(a) acredita que a utilização da certificação digital, traz segurança ao desenvolvimento dos trabalhos e além disso, é uma ferramenta importante para melhorar a gestão, ocasionando uma desburocratização e agilidade das tarefas?

( ) Sim

( ) Não

Porque_____

_____

_____

_____

_____

_____

9) Qual será o modelo de política adotado pela força no uso da assinatura digital?

_____

_____

_____

10) Foram levantados elementos jurídicos-tecnológicos na composição de um modelo de assinatura digital a ser adotado no Ministério da Defesa (Comando da Aeronáutica)?

_____

_____

_____

_____

11) Como está organizada a Infra-estrutura de chaves públicas do Ministério da Defesa (Comando da Aeronáutica)?

_____

_____

_____

_____

12) Como obter o certificado digital no Ministério da Defesa (Comando da Aeronáutica)?

_____

_____

_____

_____

13) Quais as vantagens da utilização da certificação digital no Ministério da Defesa (Comando da Aeronáutica)?

_____

_____

_____

_____

14) Em que sistemas atualmente empregados no COMAER o senhor(a) vislumbra a aplicação de certificação digital?

_____

_____

_____

_____

15) Que ação o senhor(a) tomaria para disseminar o uso de certificação digital no âmbito do COMAER?

_____

_____

_____

_____

_____

16) Qual a sua perspectivava quanto a emprego militar de certificados digitais?

_____

_____

_____

_____

_____