IMPLEMENTAÇÃO DA CERTIFICAÇÃO DIGITAL E DA ASSINATURA ELETRÔNICA NO ÂMBITO DO COMAER

Fábio Barbosa **Laureano** Luiz Al CFOE COM
Márcio Vieira Al CFOE COM

Cláudio Marcelo **Albuquerque** Nascimento Silva 1º Ten QOENG CMP[1]

RESUMO

Este artigo tem caráter informativo acerca da necessidade de se implantar um sistema de certificação digital e assinatura eletrônica no âmbito do COMAER, uma preocupação do Alto Comando. Atualmente, o CCA-BR é o responsável pela implantação de infraestrutura de Chaves Públicas no âmbito do COMAER. Há estimativas de que, ainda este ano, os integrantes do COMAER possam usufruir da funcionalidade que a assinatura eletrônica pode proporcionar, encurtando o tempo burocrático necessário e mantendo o mesmo grau de integridade e autenticidade dos documentos dentro do COMAER.

Palavras-chave: Certificado digital. Assinatura eletrônica. Integridade. Autenticidade.

[1] Chefe da Assessoria da Segurança da Informação e Chefe da Assessoria da Certificação Digital do CCA-BR.

1 INTRODUÇÃO

Entre as diversas tecnologias existentes, as telecomunicações têm se desenvolvido vertiginosamente. Surgiram com o advento do telex - transmissão e recepção de informações com a codificação Morse de caracteres, utilizando-se de tons curtos e longos de frequência audível e o homem maravilhou-se com a transmissão/recepção de informações em longas distâncias.

A telefonia veio, então, para que pudéssemos veicular voz e, assim, encurtar o tempo entre emissor e receptor de uma comunicação. O telefone celular apareceu e solucionou o problema da mobilidade dos interlocutores. Houve, em seguida, o grande salto tecnológico com as redes de computadores, o que viabilizou a globalização e a rápida troca de informações entre quaisquer usuários que desejassem interagir.

Entretanto, todas as formas de se comunicar, transferindo voz, texto, imagem, enfim, qualquer tipo de informação, necessitam de mecanismos que tratem de garantir sigilo, quando for o caso.

Muitas instituições (por exemplo, as financeiras e comerciais) já se utilizam de técnicas que permitem uma confiável tramitação de informações, garantindo a **confidencialidade** (restrição de acesso – somente pessoas autorizadas têm acesso à informação), a **integridade** (informação inalterada no destino), a **autenticidade** (garantia da autoria da mensagem) e o **não repúdio** (não negação de autoria). Uma Força Armada necessita, ainda mais, de tais garantias.

Sendo assim, a informação que atualmente tramita pelos meios eletrônicos no Comando da Aeronáutica (COMAER) requer cuidados para que a confidencialidade, a autenticidade, a integridade e o não repúdio estejam garantidos. É preocupante a mínima hipótese de que possa haver uma alteração ou interceptação indevida de uma informação trocada entre um emissor e um receptor. Por exemplo: o Comando da Aeronáutica realiza diversos exercícios operacionais no território brasileiro por meio de seus Esquadrões de Aviação, de Comunicação, organizados às vezes em Forças

Combinadas, essas envolvendo o Comando da Marinha e/ou o Comando do Exército. Durante o curso desses exercícios operacionais, os Comandantes das Forças necessitam comunicar-se com outros órgãos operacionais das Forças Armadas ou com entidades governamentais. Essas informações veiculadas por meio eletrônico, durante um exercício de campanha, são de caráter estratégico e requerem a confidencialidade, a autenticidade, a integridade e o não repúdio.

Há técnicas que podem ser implementadas visando ao impedimento da possibilidade de alteração de uma informação, assim como da interceptação, mas o principal é o estabelecimento de Políticas de Segurança da Informação nas Organizações Militares. A certificação e a assinatura digitais são componentes e aliadas desta política.

O escopo deste artigo é, pois, ressaltar a necessidade do emprego da Certificação Digital e da Assinatura Digital nas mensagens de correio eletrônico e nos diversos sistemas do COMAER, tais como o Sistema Integrado de Logística de Material e de Serviços (SILOMS), Sistema de Gestão de Pessoal (SIGPES), Sistema de Gerenciamento Eletrônico de Documentos (SGED) ou Sistema Informatizado de Gestão Arquivística e Documentos da Aeronáutica (SIGADAER).

2 TEORIA BÁSICA DE CRIPTOGRAFIA SIMÉTRICA, ASSIMÉTRICA E FUNÇÕES DE HASH

2.1 Criptografia

Criptografia (do Grego *kryptós*, "escondido" e *gráphein*, "escrita") é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de modo que seja desvendada apenas por seu destinatário (detentor de uma "chave secreta"), o que a torna difícil de ser lida por alguém não

autorizado. A criptografia é parte de um campo de estudos que trata das comunicações secretas, usadas, entre outras finalidades, para:

a) autenticar a identidade de usuários;

b) prover o sigilo de comunicações pessoais e de transações comerciais e bancárias;

c) garantir a integridade de transferências eletrônicas de fundos.

Uma mensagem codificada por um método de criptografia deve ser privada, ou seja, somente aquele que enviou e aquele que recebeu devem ter acesso ao conteúdo da mensagem. Além disso, uma mensagem deve permitir ao recebedor identificar se ela foi ou não modificada e deve, também, poder ser assinada, isto é, a pessoa que a recebeu deve ter a possibilidade de verificar se o remetente é mesmo a pessoa que diz ser.

Os métodos de criptografia atuais são seguros e eficientes e baseiam-se no uso de uma ou mais chaves. Uma chave é um pedaço de informação que controla a operação de um algoritmo de criptografia. Atualmente, os métodos criptográficos podem ser subdivididos em duas grandes categorias, de acordo com o tipo de chave utilizada: a criptografia simétrica e a criptografia assimétrica.

A criptografia simétrica consiste em se utilizar uma única chave para a criptografia (emissor) e descriptografia (receptor) da mensagem. A chave deve ser conhecida por ambos e deve ser informada por um meio seguro. Entretanto, caso essa chave seja interceptada, o sigilo da mensagem estará comprometido. Para resolver tal problema, surgiram os algoritmos de criptografia assimétrica (de chave pública e privada).

Exemplos que combinam a utilização dos métodos de criptografia simétrica e assimétrica são as conexões seguras, estabelecidas entre o *browser* de um usuário e um *site*, em transações comerciais ou bancárias via *web*. Essas conexões seguras via *web* utilizam o método de criptografia simétrica, implementado pelo protocolo SSL (*Secure Socket Layer*), segundo o qual o *browser* do usuário precisa informar ao *site* qual será a chave simétrica, utilizada na conexão segura, antes de iniciar a transmissão de dados

sigilosos. Para isso, o *browser* obtém a chave pública da instituição que mantém o *site*. Então, ele utiliza essa chave pública para codificar a chave simétrica e enviá-la como uma mensagem para o *site*, contendo a chave simétrica a ser utilizada na conexão segura. O *site*, por sua vez, utiliza sua chave privada para decodificar a mensagem e identificar a chave simétrica que será utilizada. A partir desse ponto, o *browser* do usuário e o *site* podem transmitir informações, de forma sigilosa e segura, por meio da utilização do método de criptografia de chave simétrica.

2.2 Funções de HASH

A função de HASH unidirecional extrai um trecho de qualquer texto simples e, a partir dele, calcula uma *string* de *bits* de tamanho fixo. Essa função de HASH geralmente é chamada sumário de mensagens.

As funções de HASH unidirecionais são como impressões digitais: pequenos pedaços de dados que podem servir para identificar objetos digitais muito maiores; são funções públicas, sem qualquer chave envolvida. Elas se chamam unidirecionais devido à sua natureza matemática. Pode-se calcular o HASH unidirecional de qualquer coisa. No entanto, dado, por exemplo, o HASH de um texto de uma revista, é computacionalmente inviável criar outro texto que tenha o mesmo valor ou derivar do texto original da revista.

As funções de HASH também oferecem uma medida de autenticação e verificação de integridade. Se é feito o *download* de um livro pela internet, não há como saber se as palavras escritas são do autor ou se alguém mais as alterou. No entanto, se for entregue o valor de HASH do livro , pode-se montar o livro e comparar o resultado com o HASH dado. Se eles combinarem, isso indica que o livro está inalterado.

As funções de HASH possuem uma grande faixa de aplicações na criptografia e na segurança do computador. Elas são essenciais para algoritmos de assinatura digital e são a ferramenta isolada mais útil na caixa de ferramentas do criptógrafo.

Para mensagens cuja integridade é importante, mas cujo conteúdo não é secreto, o esquema do exemplo anterior é bastante utilizado. Por um custo relativamente pequeno em computação, ele garante que as modificações feitas na mensagem de texto simples em trânsito possam ser detectadas com probabilidades muito grandes, ou seja, qualquer alteração no conteúdo da mensagem será percebida através da função HASH.

3 ICP - CONTEXTUALIZANDO AS TÉCNICAS DE CRIPTOGRAFIA E EXEMPLOS

3.1 Assinatura digital

A assinatura digital utiliza técnicas de criptografia assimétrica e funções de HASH, ou seja, uma assinatura digital nada mais é que o HASH de uma mensagem criptografada com a chave privada do remetente da mensagem.

Para exemplificar, utilizaremos a função SHA-1 (função HASH padrão nos EUA, em um passado recente). Quando Laura deseja enviar para Maria uma mensagem não secreta e assinada, sua mensagem de texto simples é colocada no algoritmo SHA-1 para se obter um HASH. Em seguida, Laura assina o HASH com a sua chave privada e envia a mensagem de texto simples e o HASH assinado para Maria. Depois de receber a mensagem, a própria Maria calcula o HASH SHA-1 e também aplica a chave pública de Laura ao HASH assinado para obter o HASH original. Se as duas corresponderem, a mensagem será considerada válida.

É importante ressaltar que a segurança do método baseia-se no fato de que a chave privada é conhecida apenas por seu dono e que o fato de assinar uma mensagem não significa gerar uma mensagem sigilosa. Para o exemplo anterior, se Laura quisesse assinar a mensagem e ter certeza de que apenas Maria teria acesso a seu conteúdo, seria preciso codificá-la com a chave pública de Maria, depois de assiná-la.

3.2 Certificado Digital

O certificado digital é um arquivo eletrônico que contém informações a respeito de uma dada pessoa, um equipamento ou uma organização e sua chave pública, as quais, combinadas, são ratificadas pela assinatura digital de uma entidade presumidamente confiável denominada Autoridade Certificadora. Esse arquivo pode estar armazenado em um computador ou em outra mídia, como um *token* ou *smart card*.

Exemplos semelhantes a um certificado digital são o CNPJ, RG, CPF e a carteira de habilitação de uma pessoa. Cada um deles contém um conjunto de informações que identificam a instituição, a pessoa e a autoridade (no caso desses exemplos, os órgãos públicos). Algumas das principais informações encontradas em um certificado digital são:

a) dados que identificam o dono (nome, número de identificação, estado etc);

b) nome da Autoridade Certificadora (AC) que emitiu o certificado;

c) o número de série e o período de validade do certificado; e

d) a assinatura digital da AC.

O objetivo da assinatura digital no certificado é indicar que uma outra entidade (a Autoridade Certificadora) garanta a veracidade das informações nele contidas.

4 ICP-BRASIL E SUA LEGISLAÇÃO

Ao tratar neste artigo sobre Segurança da Informação, é necessário ressaltar a importância do Projeto ISO 27001, o qual se encontra sob a direção não só do Subdepartamento de Tecnologia de Informação (SDTI) / Departamento de Controle do Espaço Aéreo (DECEA) / Estado Maior da Aeronáutica (EMAER), mas também dos elos especializados de tecnologia da informação do COMAER, que buscam obter a certificação ABNT ISO/IEC 27001:2006. A aderência a essa norma implica que o

COMAER adote padrões rígidos de segurança da informação e que se submeta a auditorias frequentes, demonstrando que o Órgão comprovadamente gera, implementa e mantém um Sistema de Gestão de Segurança da Informação (SGSI) que garanta os requisitos de confidencialidade, integridade, disponibilidade e não repúdio. Um SGSI garante também continuidade dos serviços críticos balizados nos processos e medidas de segurança preconizados pela referida norma de referência mundial.

É necessária, portanto, a implementação de uma entidade geradora de certificados digitais no âmbito do COMAER. Com relação às Autoridades Certificadoras (AC) e às Autoridades Registradoras (AR), faz-se mister comentar sobre a Infraestrura de Chaves Públicas Brasileira (ICP-Brasil). A ICP-Brasil é a primeira autoridade da cadeia de certificação, logo é a AC-Raiz, é mantida pelo Instituto Nacional de Tecnologia de Informação (ITI), uma autarquia federal vinculada à Casa Civil da Presidência da República. Abaixo da AC-Raiz, existe uma estrutura organizacional hierarquizada linear a qual contém outras Acs, sendo estas de primeiro nível e assim por diante.

A implantação do sistema nacional de certificação digital da ICP-Brasil teve início a partir da Medida Provisória 2200-2, de 24 de agosto de 2001. Essa Medida estabelece a presunção legal, para os documentos em meio digital, assinados com um certificado digital integrante da ICP-Brasil. O COMAER está em processo de adequação da sua infraestrura de certificação digital junto às normas preconizadas pela ICP-Brasil, e o Centro de Computação da Aeronáutica (CCA), localizado em Brasília, conforme diretriz contida na NSCA 7-6, é responsável por esse processo, bem como pela incorporação de diversos recursos de criptografia aos sistemas corporativos do COMAER.

5 PROCESSO DE CREDENCIAMENTO DO COMAER JUNTO A ICP-BRASIL

5.1 Autoridade Registradora (AR)

Quando se pretende requisitar um certificado digital, a fim de garantir validade legal e identificação inequívoca a uma transação pela internet ou ao envio de uma mensagem eletrônica, é necessário que haja uma autoridade registradora interligada com a autoridade certificadora para analisar o pedido de emissão do certificado digital.

Conforme Silva (2004, p.191), uma AR pode ter duas atribuições bem definidas: verificar o conteúdo do certificado para uma AC e fornecer os mecanismos para ingresso de novos usuários na AC. Dessa forma, a AR é a responsável pela identificação de futuros integrantes da ICP.

O CCA-BR firmou parceria com o Serviço Federal de Processamento de Dados (SERPRO), por meio de um contrato de três anos, autorizado pelo Estado Maior da Aeronáutica, cuja finalidade é a realização de assessoria e consultoria ao Comando da Aeronáutica, com um custo bem abaixo da média do mercado, para emissão de certificados digitais e treinamento de agentes de registro. O CCA-BR está em fase de homologação da Autoridade Registradora do COMAER (AR-COMAER-BR). O organograma da estrutura da SERPRO na ICP-Raiz poderá ficar definido, conforme figura 1.

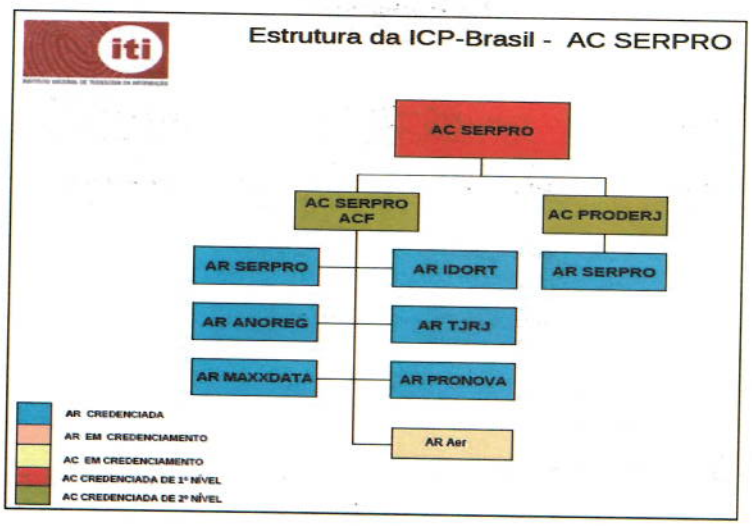

Figura 1: Estrutura da ICP-Brasil AC SERPRO
Fonte: A estrutura do ICP-BRASIL modificada após a entrada da AR-COMAER Disponível em: <www.iti.gov.br>. Acesso: 5 set. 2009.

5.2 Autoridade Certificadora (AC)

Segundo Silva (2004, p.187), a Autoridade Certificadora é a responsável por emitir os certificados digitais, os quais possuem uma forma de assinatura eletrônica da AC que os emitiu. Essa assinatura digital irá possibilitar a manutenção e a garantia da integridade, do sigilo e da segurança da informação, permitindo estabelecer uma relação de confiança com qualquer entidade que acredite na legitimidade da AC, assim como no conteúdo dos certificados emitidos e nos usuários cadastrados na AC.

Com o intuito de estar sempre na vanguarda, o Comando da Aeronáutica prepara-se para implementar a AC-COMAER (Autoridade Certificadora do COMAER), após credenciar sua AR-COMAER-BR (Autoridade Registradora). A estrutura, então, será conforme mostra a figura 2:

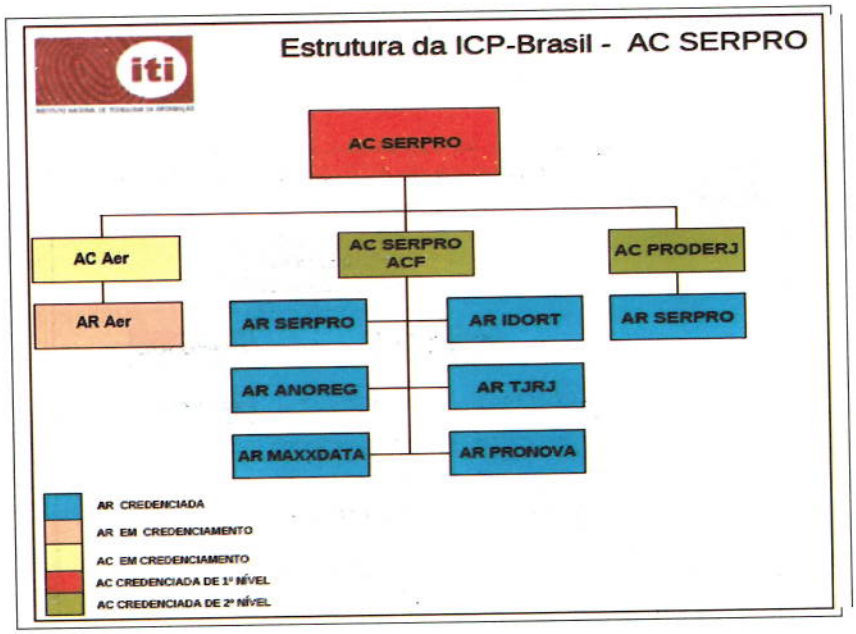

Figura 2: Estrutura da ICP-Brasil AC SERPRO
Fonte:Estrutura ICP-BRASIL modificada após a entrada da AC-COMAER e AR-COMAER. Disponível em: <www.iti.gov.br>. Acesso em: 5 set. 2009.

6 CONSIDERAÇÕES FINAIS

Este artigo remonta, brevemente, ao desenvolvimento das telecomunicações, com enfoque na importância da segurança da informação. Atualmente, não basta apenas estabelecer a comunicação entre um emissor e um receptor, mas também considerar a confidencialidade, a integridade, a autenticidade e o não repúdio da informação. Por isso, a importância dos certificados digitais e da assinatura digital que, respectivamente, por meio das Autoridades Certificadoras, atuam como "cartórios eletrônicos", e por meio do uso das chaves assimétricas, garantem a identificação e a certeza do emissor da mensagem, bem como a integridade da informação por meio da Função Hash.

É importante destacar os passos que a Força Aérea Brasileira tem realizado mediante a implantação de uma infraestrutura de chaves públicas (ICP) no âmbito do COMAER, sendo o CCA-BR o responsável por sua operacionalização. Encontra-se em fase de credenciamento uma autoridade registradora (AR-COMAER-BR), que fará a análise dos pedidos de emissão de certificados digitais, e uma autoridade certificadora AC-COMAER, que emitirá os certificados digitais.

O Comando da Aeronáutica constantemente realiza missões de caráter operacional durante as quais, necessariamente, o comandante da missão necessita dar ordens. Atualmente, não se pode considerar confiável emitir ordens por meio eletrônico; entretanto, ao se implementar a certificação digital e a assinatura eletrônica, haverá a possibilidade de ocorrer a comunicação de forma segura e confiável.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2006:** tecnologia da informação, técnicas de segurança, sistema de gestão de segurança da informação, requisitos. Rio de Janeiro: ABNT, 2006.

BRASIL. Comando da Aeronáutica. Centro de Computação. **NSCA 7-6:** diretrizes específicas para os centros de computação da Aeronáutica (CCA). Brasília: [s.n], 2005.

BRASIL. Comando da Aeronáutica. Centro de Computação. **Projeto ISO 27001.** Disponível em: <http://www.ccabr.intraer/portalccabr/index.php?option=com_content&view=article&id=168&Itemid=193>. Acesso em: 10 jul. 2009.

BRASIL. Comando da Aeronáutica. Centro de Instrução e Adaptação da Aeronáutica. **Segurança da informação**. Belo Horizonte: CIAAR, 2008. (Apostila)

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Disponível em: < http://www.iti.gov.br/twiki/bin/view/ITI/Apresentacao>. Acesso em: 30 jul. 2009.

SILVA, Lino Sarlo da. **Public Key Infrastructure - PKI**: conheça a infraestrutura de chaves públicas e a certificação digital. São Paulo: Novatec, 2004.