FACULDADE SENAI-FATESG

PÓS-GRADUAÇÃO EM
SEGURANÇA EM REDES DE COMPUTADORES

FABIANO SANTOS FLORENTINO

CERTIFICADO DIGITAL
ICP-BRASIL

Professor – Orientador: Reinaldo Borges de Freitas

Goiânia 2016

FABIANO SANTOS FLORENTINO

CERTIFICADO DIGITAL
ICP-BRASIL

Trabalho de conclusão de curso apresentado à Faculdade SENAI-FATESG, para obtenção do título de Especialista em Segurança em Rede de Computadores.

FABIANO SANTOS FLORENTINO

CERTIFICADO DIGITAL ICP-Brasil

Trabalho de conclusão de curso apresentado à Faculdade SENA-FATESG, para obtenção do título de Especialista em Segurança em Rede de Computadores.

Aprovado em _____ de _____ de 20 ____.

RESUMO

Este trabalho tem como objetivo demonstrar um breve conceito sobre crime cibernético, uma introdução sobre criptografia e suas principais técnicas de cifras simétrica e assimétrica levando em consideração o uso de certificado digital e assinatura digital. Uma introdução sobre PKI (*Public-Key Infrastructure*) e também a infraestrutura de chave pública brasileira (ICP-Brasil), sua legislação, como é regulamentada e seus principais documentos que regem toda a estrutura brasileira de certificação digital. Demonstrar uma técnica que pode ser usada com certificado digital e assinatura digital para mitigar possíveis fraudes bancárias.

OBJETIVO

Este documento tem como objetivo, abordar quais são as técnicas mais comuns de crime cibernético bem como as fraudes eletrônicas utilizadas. Um breve conceito sobre criptografia e suas principais características. O uso do certificado digital, principais características, as informações que ele carrega, meios onde são armazenados e seu prazo de validade. Uma introdução a PKI (*Public-Key Infrastructure*), infraestrutura de chave pública. Apresentar a infraestrutura de chave pública brasileira ICP-Brasil, suas principais características, sua legislação envolvida para fazer parte dela. O conceito de PKI com suas principais características e funcionalidades. E com base nessa infraestrutura demonstrar uma pratica que pode dificuldade ainda mais a fraude eletrônica por meio de assinatura digital.

LISTA DE ABREVIATURAS

AC-Raiz – Autoridade Certificadora Raiz

AC – Autoridade Certificadora

ACT – Autoridade Certificadora do Tempo

ICP-Brasil – Infraestrutura de Chaves Publicas Brasileira

ITI – Instituto de Tecnologia da Informação

LCR – Lista de Certificados Revogados

DPC – Declaração de pratica de Certificado

LISTA DE FIGURAS

LISTA DE TABELAS

Sumário

1 Introdução

Hoje os bancos oferecem vários serviços diretos na internet, facilitando o dia à dia e também aproximando mais o cliente (usuário) ao meio digital, com isso, os bancos disponibilizam serviços como o pagamento de boletos, transferência entre banco e contas do mesmo banco, solicitar crédito, pagar débitos entre outros serviços, todos esses serviços não passam de transações bancárias que são feitas pelo cliente, visando uma melhor segurança quanto ao uso desses recursos podemos utilizar o certificado digital para garantir que toda transação executada é de fato executada pelo cliente (usuário) daquela conta bancária. O trabalho irá apresentar as técnicas mais recentes quanto a tentativa de fraude eletrônica, será apresentando o conceito por traz da certificação digital como a criptografia utilizada no processo de geração de um certificado, a legislação da ICP-Brasil que regulamenta todo esse processo, se o uso do certificado digital junto com a ICP-Brasil poderá trazer mais segurança para as transações eletrônicas a assinatura digital parte do processo que faz o uso do certificado garantindo a autenticidade da transação e por fim uma técnica utilizada nas transações bancárias que pode vir a mitigar essas ações quanto a fraude eletrônica bancária.

2 Crime Cibernético

Segundo a Symantec (2016): Tal como a criminalidade tradicional, a cibercriminalidade pode assumir muitas formas e pode ocorrer quase a qualquer hora ou lugar. Os criminosos cibernéticos usam métodos diferentes segundo suas habilidades e seus objetivos. Esse fato não deveria ser surpreendente, afinal, o crime cibernético é nada mais que um "crime" com um ingrediente "informático" ou "cibernético".

Segundo a Symantec (2016): O Tratado do Conselho Europeu sobre Crime Cibernético usa o termo "cibercrime" para definir delitos que vão de atividades criminosas contra dados até infrações de conteúdo e de copyright [Krone, 2005]. No entanto, outros autores [Zeviar-Geese, 1997-98] sugerem que a definição é mais ampla e inclui atividades como fraude, acesso não autorizado, pornografia infantil e cyberstalking (assédio na Internet). O Manual de Prevenção e Controle de Crimes Informáticos das Nações Unidas inclui fraude, falsificação e acesso não autorizado [Nações Unidas, 1995] em sua definição de cibercrime.

2.1 Fraude Eletrônica

Com o aumento do uso da Internet e do correio eletrônico (e-mail), tornou-se grande o número de pessoas mal-intencionadas que tentam utilizar esses meios para realizar fraudes. Por isso, a informação é a melhor maneira de se prevenir contra estes tipos de ações.

Segundo Cert.br (2012): Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial e, por este motivo, golpistas vêm concentrando esforços na exploração de fragilidades dos usuários. Utilizando técnicas de engenharia social e por diferentes meios e discursos, os golpistas procuram enganar e persuadir as potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas.

De posse dos dados das vítimas, os golpistas costumam efetuar transações financeiras, acessar sites, enviar mensagens eletrônicas, abrir empresas fantasmas e criar contas bancárias ilegítimas, entre outras atividades maliciosas.

Muitos dos golpes aplicados na Internet podem ser considerados crimes contra o patrimônio, tipificados como estelionato. Dessa forma, o golpista pode ser considerado um estelionatário.

2.1.1 Engenharia Social

Segundo Santander (2016): A Engenharia Social consiste numa série de técnicas utilizadas por pessoas mal-intencionadas para obter informações sigilosas de usuários, como senhas, número de cartão de crédito etc. Dentre essas técnicas, podemos destacar as mais usadas na Internet: o scam e o phishing. O scam é uma técnica que visa obter informações por e-mail, será explicada mais abaixo. O phishing também é uma técnia de captura de informações por e-mail através de links, também será tratada em um tópico. Solicitação de informações pessoais por telefone por falsos atendentes de serviços seja ele telefonico, marketing, tvs à cabo, pessoas se passando por falsos entregadores entre outros. Essas técnicas utilizam como premissa a ingenuidade e a curiosidade das pessoas para enganar e tirar proveito próprio.

2.1.2 Phising

Segundo Santander (2016): O phishing (do inglês, fishing, que significa pescar) é uma das táticas usadas por fraudadores para tentar capturar dados confidenciais de usuários da Internet. É enviado ao usuário um e-mail com uma mensagem falsa. Geralmente essas mensagens utilizam pretextos como brindes, promoções etc. ou até mesmo situações que requerem sua atenção. Para dar credibilidade as mensagens, esses e-mails, em sua grande maioria, utilizam a imagem de uma empresa idônea ou de um site verdadeiro. O objetivo é sempre de enganar o usuário e induzi-lo a clicar em um link contido na mensagem.

2.1.3 Programas Espiões

São programas que ficam escondidos no computador, com o objetivo de controlar, espionar e coletar informações e hábitos de navegação do usuário, sem que ele saiba. Além disso, podem deixar o computador mais vulnerável a ataques.

2.1.4 Scam

Segundo Santander (2016): É o nome dado à técnica de enganar usuários de Internet por meio de falsas mensagens eletrônicas (e-mails). Geralmente, essas mensagens possuem a aparência de fontes segura, pois em sua grande maioria simulam uma comunicação oficial de uma empresa conceituada.

A diferença dessas falsas mensagens para os comunicados oficiais das empresas é que elas são sempre acompanhadas por link ou por programas espiões anexos à mensagem. Os fraudadores inventam as mais mirabolantes estórias (promoções, prêmios, brindes, alertas etc.) para convencê-lo a clicar no link contido na mensagem ou a executar o programa anexo.

2.1.5 Roubo de Identidade

Segundo Santander (2016): O roubo de identidade ocorre quando alguém usa suas informações pessoais como: nome, RG, CPF, senhas, nº. de cartão de crédito ou débito, número de conta corrente etc. para cometer fraudes. Isso pode ocorrer, por exemplo, quando uma pessoa tem seu cartão de crédito roubado ou tem capturado os dados contidos no cartão. De posse dessa informação, o golpista pode falsificar um cartão de crédito. Eles podem reproduzi-lo com um design "similar" ao original, mas com os dados de um cartão verdadeiro, conseguido de alguma forma fraudulenta. Este é apenas um exemplo. O roubo de identidade envolve vários crimes contra a privacidade, incluindo a falsificação de documentos pessoais.

3 Criptografia

3.1 Conceito

Segundo Edward, Fábio e Rodolfo (2010): A criptografia pode ser entendida como um conjunto de métodos e técnicas para cifrar ou codificar informações legíveis através de um algoritmo, convertendo um texto original em um texto ilegível, sendo possível através do processo inverso recuperar as informações originais.

3.2 Tipos de Criptografia

Existem dois tipos de criptografia: simétrica e assimétrica. A criptografia simétrica é baseada em algoritmos que dependem de uma mesma chave, denominada chave secreta, que é usada tanto no processo de cifrar quanto no de decifrar o texto. Para a garantia da integridade da informação transmitida é imprescindível que apenas o emissor e o receptor conheçam a chave. Já a criptografia assimétrica utiliza um par de chaves diferentes entre si, que se relacionam matematicamente por meio de um algoritmo, de forma que o texto cifrado por uma chave, apenas seja decifrado pela outra do mesmo par.

Segundo Cert.br (2012): **Criptografia de chave simétrica:** também chamada de criptografia de chave secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados. Casos nos quais a informação é codificada e decodificada por uma mesma pessoa não há necessidade de compartilhamento da chave secreta. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, e necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave). Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA.

Segundo Cert.br (2012): **Criptografia de chaves assimétricas:** também conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma publica, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodifica-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não-repudio. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um smartcard ou um token. Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ECC e Diffie-Hellman.

3.3 Padrões e Algoritmos Criptográficos da ICP-Brasil

A ICP-Brasil junto com o comitê gestor, determinaram o uso dos seguintes tipos de algoritmos para os certificados das autoridades certificadoras e usuário final conforme o documento normativo DOC-IP-01.01.

Geração de Chaves Assimétricas de AC	
Formato	Padrão PKCS#10
Algoritmo	RSA ou ECC-Brainpool (conforme RFC 5639)
Tamanho da Chave	RSA 2048, RSA 4096, brainpoolP512r1

TABELA 1 - Padrões e Algoritmos Criptográficos para Autoridade Certificadora

Geração de Chaves Assimétricas de Usuário Final	
Formato	Padrão PKCS#7
Algoritmo	RSA ou ECC-Brainpool (conforme RFC 5639)
Tamanho da Chave	RSA 2048, RSA 4096, brainpoolP512r1
Tamanho de chave A1, A2, A3, A CF-e-SAT, S1, S2, S3, T3	RSA 1024, RSA 2048, brainpoolP256r1
Tamanho da chave A4, S4, T4	RSA 2048, RSA 4096, brainpoolP512r1

TABELA 2 - Padrões e Algoritmos Criptográficos para Usuário Final

4 Certificado Digital

Segundo Cert.br (2012): O certificado digital e um registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave publica. Ele pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um site Web) e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital.

Segundo o Instituto de Tecnologia da Informação (ITI) (2016): O certificado digital da ICP-Brasil, além de personificar o cidadão na rede mundial de computadores, garante, por força da legislação atual, validade jurídica aos atos praticados com o seu uso. A certificação digital é uma ferramenta que permite que aplicações como comércio eletrônico, assinatura de contratos, operações bancárias, iniciativas de governo eletrônico, entre outras, sejam realizadas. São transações feitas de forma virtual, ou seja, sem a presença física do interessado, mas que demanda identificação clara da pessoa que a está realizando pela intranet.

4.1 Tipos de certificado

Cada AC tem sua respectiva política quanto a necessidade da entidade (pessoa, processo e ou equipamento). Esses tipos determinam a área de atuação do certificado (Pessoa Física ou Jurídica), tipo de entidade, qual sua finalidade e tempo validade.

4.2 Principais informações de um certificado digital

Os certificados emitidos pela AC responsável, segundo a PC (Política de Certificação), deverão estar em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

4.2.1 Número(s) de versão

Todos os certificados emitidos pela AC responsável deverão implementar a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

4.2.2 Extensões de certificado

A ICP-Brasil define como obrigatórias as seguintes extensões para certificados de AC:

- **“Authority Key Identifier”, não crítica:** o campo keyIdentifier deve conter o hash SHA-1 da chave pública da AC que emite o certificado; ou seja, é a assinatura da chave criptografica da AC (Autoridade Certificadora), garantindo a integridade da informação presente no campo.
- **“Subject Key Identifier”, não crítica:** deve conter o hash SHA-1 da chave pública da AC titular do certificado; ou seja, é a assinatura da chave criptografica da parte pública do certificado.
- **“Key Usage”, crítica:** somente os bits keyCertSign e cRLSign devem estar ativados;
    - **“Certificate Policies”, não crítica:**
        - O campo policyIdentifier deve conter:
            - OID da DPC da AC titular do certificado, se essa AC emite certificados para outras ACs; ou
            - OID das PCs que a AC titular do certificado implementa, se essa AC emite certificados para usuários finais;
        - O campo policyQualifiers deve conter o endereço Web da DPC da AC que emite o certificado;
    - **“Basic Constraints”, crítica:** deve conter o campo cA=True; ou seja, o campo deve conter

uma AC válida perante a AC Raiz da hierarquia de certificados.

- **“CRL Distribution Points”, não crítica:** deve conter o endereço na Web onde se obtém a LCR (Lista de Certificados Revogados) correspondente ao certificado; ou seja, lista que contém os certificados revogados pela AC (Autoridade Certificadora).

São 11 (onze) os tipos, inicialmente previstos, de certificados digitais para usuários finais da ICP-Brasil, conforme o descrito a seguir:

4.2.3 Tipos de Certificados de Assinatura Digital

- A1
- A2
- A3
- A4
- T3
- T4
- A CF-e-SAT

4.2.4 Tipos de Certificados de Sigilo

- S1
- S2
- S3
- S4

Os tipos de certificados indicados acima, de A1 a A4 e de S1 a S4, definem escalas de requisitos de segurança, nas quais os tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos.

Certificados dos tipos de A1 a A4 e de S1 a S4, de assinatura ou de sigilo, podem, conforme a necessidade, ser emitidos pelas ACs para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações.

Certificados do tipo T3 e T4 somente podem ser emitidos para equipamentos das Autoridades de Carimbo do Tempo (ACTs) credenciadas na ICP-Brasil. Os certificados do tipo T3 e T4 estão associados aos mesmos requisitos de segurança, exceto pelo tamanho das chaves criptográficas utilizadas.

Certificados do tipo A CF-e-SAT só podem ser emitidos para equipamentos integrantes do Sistema de Autenticação e Transmissão do Cupom Fiscal Eletrônico - SAT-CF-e, seguindo a regulamentação do CONFAZ.

Outros tipos de certificado, além dos onze anteriormente relacionados, podem ser propostos para a apreciação do Comitê Gestor da ICP-Brasil – CG da ICP-Brasil. As propostas serão analisadas quanto à conformidade com as normas específicas da ICP-Brasil e, quando aprovadas, serão acrescidas aos tipos de certificados aceitos pela ICP-Brasil.

4.2.5 Formatos de nomes

O nome da AC titular de certificado, constante do campo “Subject”, deverá adotar o “Distinguished Name” (DN) do padrão ITU X.500/ISO 9594, como exemplo, da seguinte forma:

- **C = BR**
- **O = ICP-Brasil**
- **OU = nome da AC emitente**
- **CN = nome da AC titular**

4.3 Exemplo de Certificado Digital

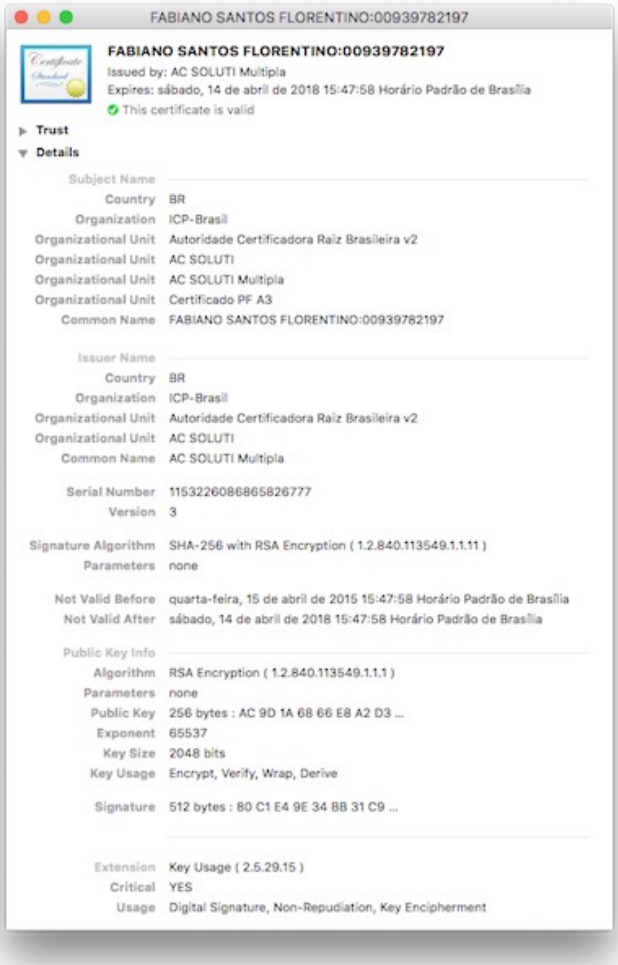

FIGURA 1 – Certificado Digital
Fonte: Próprio Certificado (2016)

4.4 Mídias Armazenadoras de Chaves Criptográficas

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A1 e S1	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima
A2 e S2	Cartão Inteligente ou Token, ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica
A3 e S3	Cartão Inteligente ou Token, ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica, ou hardware criptográfico homologado junto à ICP-Brasil
A4 e S4	Hardware criptográfico homologado junto à ICP-Brasil
T3 e T4	Hardware criptográfico homologado junto à ICP-Brasil
A CF-e-SAT	Hardware criptográfico

TABELA 1 - Mídias Armazenadoras de Chaves Criptográficas

4.5 Validade do Certificado

Os períodos máximos de validade admitidos para cada tipo de certificado previsto pela ICP-Brasil:

Tipo de Certificado	Período Máximo de Validade do Certificado (em anos)
A1 e S1	1
A2 e S2	2
A3, S3 e T3	5
A4, S4 e T4	11 (para cadeias hierárquicas completas em Curvas Elípticas)
	6 (para as demais hierarquias)
A CF-e-SAT	5

TABELA 2 – Períodos de Validade dos Certificados

4.5.1 LCR

Segundo Délio Silva Nunes (2007): As Listas de Certificados Revogados (LCR) podem ser definidas como uma estrutura de dados assinada por uma AC contendo a lista de certificados que não devem ser considerados válidos. Embora um certificado digital possua uma data para sua expiração, algumas vezes é necessário que sua validade seja negada antes do término deste prazo. Assim, um certificado pode ser revogado e, a partir deste momento, ele constará em uma lista de certificados inválidos. Uma forma de distribuição da lista de certificados revogados é através de página web. O local onde a lista de certificados revogados encontra- se é adicionado em uma extensão do certificado digital.

4.6 Caminhos da Certificação

Segundo Délio Silva Nunes (2007): Os certificados digitais são emitidos através de uma infra-estrutura de chaves públicas por uma hierarquia de Autoridades Certificadoras. O caminho de certificação é a reconstrução desta hierarquia a partir do certificado final. O caminho de certificação é necessário para determinar a confiança ou não em um certificado. Ele é formado por todos os certificados (Certificado Raiz, AC Intermediárias e Certificado Final do Usuário). A construção do caminho de certificação deve, entre outras coisas, realizar para cada certificado digital da cadeia de certificação o seguinte procedimento:

- Verificar se a cadeia do certificado esta completa. Se estiver faltando um certificado, a verificação retorna um erro;
- Verificar a validade do certificado;
- Verificar se o certificado esta revogado;
- Verificar assinatura do certificado (foi assinado pelo emissor);
- Verificar nomes (emissor do certificado igual assunto de seu emissor);
- Verificar se o certificado digital do emissor possui o valor de assinatura de certificado na extensão de uso da chave (key usage);
- Verificar se o certificado do emissor pode emitir certificado digital para outra entidade;
- Verificar se LCR é válida;
- Verificar se a LCR não está expirada;
- Verificar assinatura da LCR (pelo emissor do certificado);
- Verificar se o certificado do emissor da LCR possui o valor de assinatura de LCR na extensão de uso da chave(key usage).

4.7 Aplicabilidade

4.7.1 SSL

Globalsign (2016): A Camada de Soquetes Segura (*Secure Sockets Layer ou SSL*) e a Segurança da Camada de Transporte (*Transport Layer Security ou TLS*) são protocolos de segurança usados hoje em dia. Esses protocolos estabelecem um canal seguro entre dois computadores conectados via Internet ou uma rede interna. Em nosso cotidiano, onde a Internet desempenha um papel tão proeminente, é muito comum encontrar conexões entre navegadores e servidores web utilizando conexões de Internet não seguras, sem a presença da tecnologia SSL.

4.7.1.1 Certificado SSL Validação Extendia (EV)

O SSL EV dá mais credibilidade ao seu website comparado ao uso de um Certificado SSL da organização ou de domínio validado. Além de exibir indicadores prominentes de segurança, como tornar a barra de endereço verde e exibir o nome da sua organização, o Extended SSL possui uma gama de características singulares.

- Nível de criptografia de 2048 bits e Suporte para a Elliptic Curve Cryptography (ECC)
- Certificados assinados SHA-256
- Um único certificado protege a versão www e a versão não-www do domínio
- Compatibilidade Universal com browsers, aparelhos celulares e dispositivos móveis em geral

Certificados EV SSL estão disponíveis para todos os tipos de negócios, incluindo entidades governamentais. E também corporações e empresas de todos os portes. Um segundo conjunto de orientações, as Diretrizes de Auditoria EV, especifica os critérios segundo os quais uma Autoridade Certificadora (AC) precisa ser auditada com sucesso antes de emitir certificados EV SSL. As auditorias são repetidas anualmente para garantir a integridade do processo de emissão.

4.7.1.2 Certificado SSL (OV)

Onde a AC verifica o direito do candidato de usar um nome de domínio específico E AINDA realiza algum veto da organização. Informação adicional da empresa vetada é exibida para clientes ao clicar sobre o Selo Site Seguro, dando maior visibilidade em quem está por trás do site e o reforço da confiança associado.

4.7.1.3 Certificado SSL (DV)

Onde a AC verifica o direito do candidato de usar um nome de domínio específico. Nenhuma informação sobre a identidade da empresa é vetada e nenhuma informação é exibida além das informações de criptografia dentro do Selo Site Seguro.

4.7.2 VPN

Segundo Cert.br (2012): Do inglês *Virtual Private Network*. Termo usado para se referir a construção de uma rede privada utilizando redes publicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso a rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

4.7.2.1 OpenVPN

Segundo OpenVPN (2013): O OpenVPN é uma VPN SSL com as características que implementa o modelo OSI na camada 2 ou 3 com extensão de rede segura usando o protocolo SSL/TLS padrão da industria atual. Suporta de maneira flexível métodos de autenticação de clientes baseados em certificados, smartcards e/ou credenciais de usuário e senha.

4.8 Certificado Digital ICP-Brasil

Segundo ITI (2015): São muitas as possibilidades de aplicações da assinatura digital, dentre elas encontram-se as seguintes: comércio eletrônico, processos judiciais e administrativos em meio eletrônico, facilitar a iniciativa popular na apresentação de projetos de lei, uma vez que os cidadãos poderão assinar digitalmente sua adesão às propostas, assinatura da declaração de renda e outros serviços prestados pela Secretaria da Receita Federal, obtenção e envio de documentos cartorários, transações seguras entre instituições financeiras, como já vem ocorrendo desde abril de 2002, com a implantação do Sistema de Pagamentos Brasileiro – SPB.

O certificado digital possui muitas aplicabilidade tanto na esfera governamental quanto na privada.

4.8.1 Governo

Na esfera governamental são varias as possibilidades de uso. Abaixo alguns exemplos:

- **Governo Federal**
- **Instituto Nacional da Propriedade Industrial – INPI**
- **Receita Federal**
- **Governo Estadual e Municipal**
- **Sistema Jurídico**

4.8.2 Iniciativa privada e outros

- **Micro e pequenas Empresas:** Com o e-CPF Simples, as micro e pequenas empresas podem comprovar a identidade no meio virtual, realizar transações comerciais e financeiras com validade jurídica e trocar mensagens eletrônicas com segurança e agilidade. Também permite às empresas comprar e vender pela Internet, participar de pregões eletrônicos, fornecer ao Estado, fechar negócios e contratos de câmbio, entre outros benefícios.
- **Carteiras de identidade Profissional:** Os advogados, médicos, corretores, arquitetos e contadores possuem carteiras de identidades profissionais, emitidas pelos respectivos órgãos de classe, com certificado digital, o que permite a esses profissionais a execução de inúmeras atividades com segurança e sem a necessidade de se deslocar fisicamente.
- **Correio Eletrônico (E-mail):** Garante a identidade do emissor, a integridade e a inviolabilidade do conteúdo da mensagem enviada.

4.8.3 Vantagens para empresas e pessoas

Agilidade, redução de custos e segurança. São essas as principais vantagens da certificação digital. A certificação digital hoje permite que processos que tinham que ser realizados pessoalmente ou por meio de inúmeros documentos em papel, possam ser feitos totalmente por via eletrônica. Com isso os processos tornam-se menos burocráticos, mais rápidos e por conseguinte, mais baratos. A certificação digital garante autenticidade e integridade. O documento com assinatura digital ICP-Brasil tem a validade de um documento em papel assinado manualmente.

4.8.4 Cuidados Necessários

Segundo o ITI (2016): Primeiramente, deve-se lembrar que o certificado digital representa a “identidade” da pessoa no mundo virtual. Assim, é necessária a adoção de alguns cuidados para se evitar que outra pessoa possa fechar contratos e/ou negócios e realizar transações bancárias em nome do titular do certificado. Recomendações para o uso de um certificado digital:

- A senha de acesso da chave privada e a própria chave privada não devem ser compartilhadas com ninguém;
- Caso o computador onde foi gerado o par de chaves criptográficas seja compartilhado com diversos usuários, não é recomendável o armazenamento da chave privada no disco rígido, pois todos os usuários terão acesso a ela, sendo melhor o armazenamento em smart card ou token;

- Caso a chave privada esteja armazenada no disco rígido de algum computador, deve-se protegê-lo de acesso não-autorizado, mantendo-o fisicamente seguro. Nunca deixe a sala aberta quando sair e for necessário deixar o computador ligado. Utilize também um protetor de tela com senha. Cuidado com os vírus de computador, eles podem danificar e roubar sua chave privada;

- Caso o software de geração do par de chaves permita optar entre ter ou não uma senha para proteger a chave privada, recomenda-se a escolha pelo acesso por meio de senha. Não usar uma senha significa que qualquer pessoa que tiver acesso ao computador poderá se passar pelo titular da chave privada, assinando contratos e movimentando contas bancárias. Em geral, é bem mais fácil usar uma senha do que proteger um computador fisicamente;

- Utilize uma senha longa, intercalando letras e números, uma vez que existem programas com a função de desvendar senhas. Deve-se evitar o uso de dados pessoais como nome de cônjuge ou de filhos, datas de aniversários, endereços, telefones, ou outros elementos relacionados com a própria pessoa. A senha nunca deve ser anotada, sendo recomendável sua memorização.

5 Infraestrutura de chaves públicas brasileira (ICP-Brasil)

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. O modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o Instituto de Tecnologia da Informação (ITI), além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

5.1 Comitê Gestor ICP-Brasil

O CG ICP-Brasil tem por finalidade atuar na formulação e controle da execução das políticas públicas relacionadas à Infra-Estrutura de ChavesPúblicas Brasileira - ICP-Brasil, inclusive nos aspectos de normatização e nos procedimentos administrativos, técnicos, jurídicos e de segurança, que formam a cadeia de confiança da ICP-Brasil.

O Comitê é composto por doze membros, sendo cinco representantes da sociedade civil, integrantes de setores interessados, e sete representantes dos seguintes órgãos, indicados por seus titulares:

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

Os membros do Comitê serão designados pelo Presidente da República e, em seus impedimentos ou ausências, serão substituídos pelos seus respectivos suplentes.

Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução, por iguais e sucessivos períodos.

São convidados para participar das reuniões, em caráter permanente, dois representantes indicados pelo Conselho Nacional de Justiça – CNJ, sem direito a voto.

Poderão ser convidados para participar das reuniões, a juízo do seu Coordenador ou do próprio Comitê, técnicos e especialistas de áreas afins.

5.1.1 Secretário executivo

Renato da Silveira Martini
Diretor-Presidente do Instituto Nacional de Tecnologia da Informação
iti.gabinete@planalto.gov.br

5.1.2 Ministério da Fazenda

Titular: Fernando Nascimento Barbosa - Coordenador-Geral de Desenvolvimento Institucional de Programas de Gestão
1º Suplente: Cláudia Maria de Andrade - Coordenadora-Geral de Tecnologia da Informação

5.1.3 Ministério do Desenvolvimento, Indústria e Comércio Exterior

Titular: Amilton Mendes Junior
Suplente: Nublan Mendonça Amorim

5.1.4 Ministério do Planejamento, Orçamento e Gestão

Titular: Fernando Antonio Braga da Siqueira Junior
Suplente: José Ney de Oliveira Lima

5.1.5 Ministério da Justiça

Titular:
Suplente: Marcus Vinicius Antunes Liberato

5.1.6 Ministério da Ciência e Tecnologia

Titular: José Henrique de Lima Correia Dieguez Barreiro
Suplente: Marcos Vinícius Amorim Ferreira Guimarães

5.1.7 GSI/PR - Gabinete de Segurança Institucional

Titular: Raphael Mandarino Júnior
Suplente: Marconi dos Reis Bezerra

5.1.8 Associação Nacional de Certificação Digital - ANCD

Titular: Júlio Cesar Rogério Cosentino
Suplente: Antônio Sérgio Borba Cangiano

5.1.9 Câmara Brasileira de Comércio Eletrônico - CAMARA E-NET

Titular: Manuel Dantas Matos
Suplente: Patrícia Macedo de Paiva

5.1.10 Associação das Autoridades de Registro do Brasil - AARB

Titular: Nivaldo Cleto
Suplente: Bruno Linhares Gomes Soares

5.1.11 Sociedade Brasileira de Computação - SBC

Titular: Ricardo Felipe Custódio
Suplente: Ricardo Dahab

5.1.12 CNJ – Conselho Nacional de Justiça

Convidado: Braúlio Gabriel Gusmão
Convidado: Flávio Abreu Amorim

5.2 Como Funciona

Segundo William Stalling (2014): A RFC 4949 (*Internet Security Glossary*) define a infraestrutura de chave pública (PKI, do acrônico em inglês para *Public-Key Infrastructure*) como o conjunto de hardware, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revogar certificados digitais com base na criptografia assimétrica. O objetivo principal para desenvolver uma PKI é permitir a aquisição segura, conveniente e eficiente de chaves públicas.

Segundo Hugo (2008): A infra-estrutura de Chaves Públicas (PKI) é um sistema que utiliza mecanismos de segurança baseados na criptografia de chaves públicas para promover a autenticação, a confidencialidade, a integridade e o não repúdio de informações. Esta infra-estrutura surge como uma solução para garantir a segurança na troca de informações sigilosas em ambientes inseguros, como a Internet. Dentre as atividades que exploram intensamente esta tecnologia, podemos citar o acesso a bancos online (Internet Banking), sítios de compra e venda (e- commerce), a identificação de funcionários em uma empresa e a proteção de documentos confidenciais.

5.2.1 AC Raiz

Segundo ITI (2016): A Autoridade certificadora Raiz da ICP-Brasil (AC-Raiz) é a primeira autoridade da cadeia de certificação. Executa as políticas de certificados e normas técnicas e operacionais aprovadas pelo comitê gestor. Compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível subsequente ao seu.

5.2.1.1 Versões do Certificado da AC Raiz

O controle das versões dos certificados da AC Raiz é feito através da DCP da AC Raiz documento DOC-ICP-01 - versão 4.5

- Certificado da AC Raiz da ICP-Brasil - Expirado em 30/11/2011

- Certificado da AC Raiz da ICP-Brasil v1
  - Resolução nº 49, de 03.06.08 (versão 3.0)
  - Item alterado na DCP: 1.1.1, 1.1.2, 2.1.1, 2.1.4.2, 2.6.1.1, 2.6.3.1, 2.8.3, 4.4.1.4, 4.4.1.5, 4.4.1.7, 4.4.9, 4.4.10, 5.2.1.6, 6.1.1.1, 6.1.1.3, 6.1.8, 6.1.9, 6.2, 6.2.1, 6.2.2, 6.2.4.1, 6.2.6, 6.2.7, 6.2.8, 6.2.9, 6.3.2, 6.4.1, 6.4.2, 6.5.1.1, 6.6.2, 6.7, 6.8, 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.3, 7.3.1, 7.3.2
  - tem alterado ou excluído em função da geração da segunda chave da AC Raiz

- Certificado da AC Raiz da ICP-Brasil v2
  - Resolução 81, de 17.06.2010 (versão 4.1)
  - Item alterado na DPC: 7.1.2, 7.1.4, 7.2.4
  - Descrição: Inclusão das cadeias V2 e V3

- Certificado da AC Raiz da ICP-Brasil v3 - Revogado em 26/02/2014
  - Resolução 81, de 17.06.2010 (versão 4.1)
  - Item alterado na DPC: 7.1.2, 7.1.4, 7.2.4
  - Descrição: Inclusão das cadeias V2 e V3

- Certificado da AC Raiz da ICP-Brasil v4
  - Resolução 104, de 23 de abril de 2015 (Versão 4.4)
  - Item alterado na DPC: 7.1.2, item c) , 7.1.4, item e)
  - Descrição: Inclusão da cadeia V4

- Certificado da AC Raiz da ICP-Brasil v5 - Emitido em 02/03/2016
  - Resolução 116, de 09 de dezembro de 2015 (Versão 4.5)
  - Item alterado na DPC: 4.4.3.3, 4.4.9, 7.1.2, alínea c) e 7.1.4, alínea f)
  - Descrição: Inclusão da cadeia V5, Revogação de certificados pela AC Raiz, LCR final e flexibilização da frequência de emissão da LCR da AC Raiz.

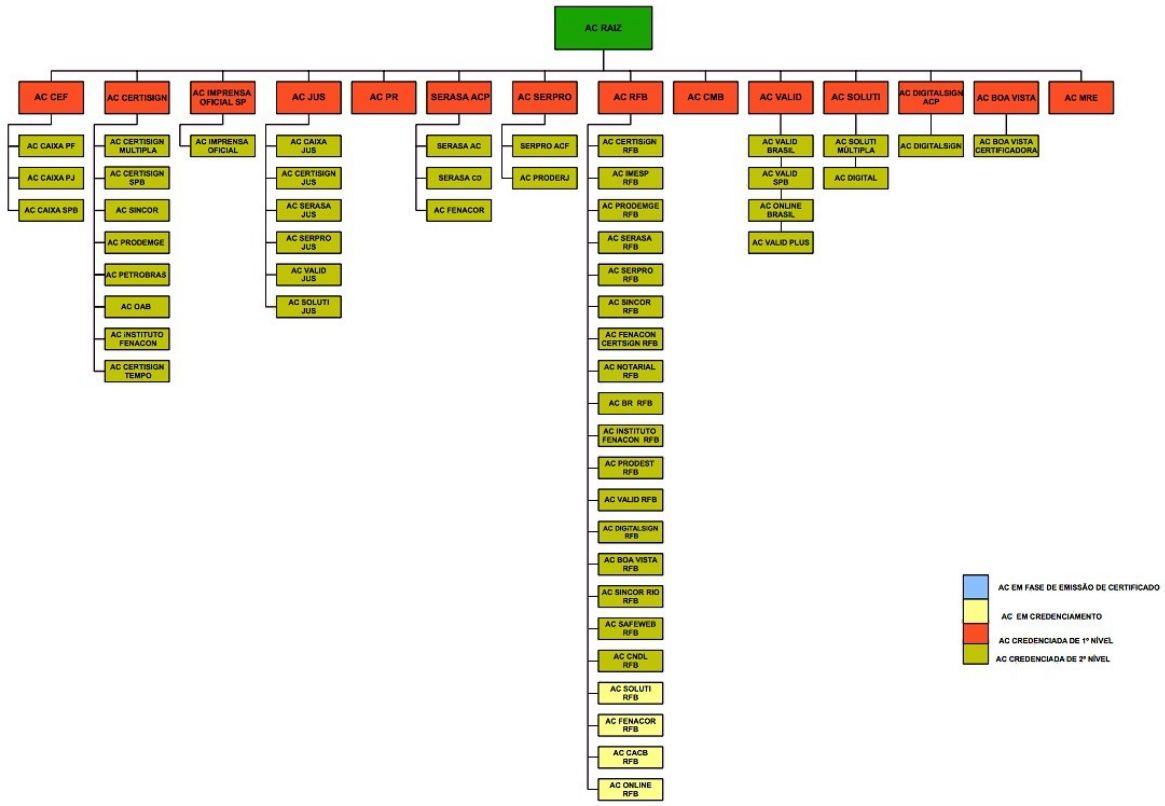

FIGURA 2 – Primeiro Nível da Estrutura da ICP-Brasil
Fonte: http://www.iti.gov.br (2016)

FIGURA 3 – Principais Autoridades Certificadoras da ICP-Brasil
Fonte: http://www.iti.gov.br (2016)

5.2.2 Autoridade Certificadora

Segundo o ITI (2015): A Autoridade Certificadora é uma entidade pública ou privada, pertencente à cadeia da ICP-Brasil que tem como responsabilidade emitir, distribuir, renovar, revogar e gerenciar certificados digitais. É de sua responsabilidade verificar se o titular possui a chave privada correspondente à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração de identidade do titular que possui um par de chaves (publica/privada). A AC tem também como obrigação por parte de suas atividades emitir lista de certificados revogados (LCR) e manter seu registro de operação sempre obedecendo as práticas definidas na declaração de praticas de certificados (DPC), e deve ainda fazer cumprir a política de segurança nas autoridades registradoras (AR) vinculadas à sua cadeia, a fim de garantir a autenticidade e identificação realizada.

Segundo Emilio Tissato e Paulo Lício (2010): Autoridades Certificadoras (CA), têm a função de criar, manter e controlar todos os certificados por ela emitidos, incluindo a invalidação de certificados comprometidos ou expirados.

5.2.3 Autoridade Certificadora do Tempo

Segundo o ITI (2015): Uma Autoridade Certificadora do Tempo (ACT) é uma entidade na qual os usuários de serviços de carimbo do tempo confiam para emitir carimbos do tempo. A ACT tem a responsabilidade geral pelo fornecimento do carimbo do tempo , conjunto de atributos fornecidos pela parte confiável do tempo que, associado a uma assinatura digital, consegue provar sua existência em determinado período. Na prática, um documento é produzido é um hash e gerado. Em seguida, ele recebe os atributos ano, mês, dia , hora, minutos e segundos, atestado na forma de assinatura realizada com o certificado digital da ACT servindo assim para comprovar sua autenticidade. A ACT atesta não apenas a questão temporal de uma transação, mas também a integridade de seu conteúdo.

Segundo CryptoID (2015): Carimbo do Tempo é um conceito genérico que engloba termos como: datação eletrônica, carimbo de tempo, selo cronológico digital, carimbo digital, protocolos digitais e outros.

Basicamente, a função do Carimbo do Tempo é comprovar a ocorrência de um evento no meio eletrônico em um determinado instante que na maioria dos casos requer eficácia probatória e adicionalmente o documento ao receber o Carimbo do Tempo passa ter informações protegidas contra alterações, assegurando que aquele é o conteúdo final naquele dia e hora.

Carimbo do Tempo é uma sequência de caracteres, indicando a data e ou o tempo em que um determinado evento ocorreu. Estes dados são normalmente apresentados em um formato consistente, permitindo fácil comparação de dois diferentes registros e acompanhamento do progresso ao longo do tempo.

O recurso do Carimbo do Tempo confere o caráter de temporalidade e tempestividade aos atos praticados no meio eletrônico. A temporalidade está relacionada ao período de tempo e ao gerenciamento de documentos eletrônicos uma vez que está determinando o ciclo de vida do documento, e a tempestividade registra o momento exato do ato praticado.

As Autoridades Certificadoras do Tempo – ACT’s são as entidades responsáveis pela emissão do Carimbos do Tempo no Brasil, que seguem normativas e padrões determinados pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira – CG ICP-Brasil. O carimbo do tempo registra o horário sincronizado aos relógios dos SCTs – Servidores de Carimbo do tempo (SCTs) e são auditados e sincronizados por Sistemas de Auditoria e Sincronismo (SAS).

5.2.4 Autoridade de Registro

Segundo o ITI (2015): A Autoridade de Registro faz o gerenciamento da interface entre o usuário e a Autoridade Certificadora. Junto da cadeia de sua AC tem como responsabilidade o recebimento, validação encaminhamento de solicitações de emissão ou revogação dos certificados emitidos de forma presencial dos seus solicitantes. Também é de sua responsabilidade manter registros de suas operações.

Segundo Délio Silva Nunes (2007): Uma Autoridade de Registro (AR) provê uma interface entre um usuário e uma AC. Ela é responsável por conferir as informações do usuário e enviar a requisição do certificado para a AC. A qualidade do processo de conferência das informações determina o nível de confiança que deve ser atribuído ao certificado.

5.3 Legislação

5.3.1 Principais Documentos

Os DOC-ICP são uma versão das resoluções da ICP-Brasil em vigor, organizadas de forma a facilitar a leitura e compreensão daquele que as estuda. Eles são a compilação das resoluções da ICP-Brasil, apresentando porem apenas o conteúdo referente a determinada regra imposta por esta resolução, ao invés da versão completa, como foi publicada no Diário Oficial da União. Cada DOC-ICP corresponde a uma resolução vigente.

Código	Tipo de Documento	Forma de Aprovação
DOC-ICP-nn	Documento da ICP-Brasil	Resolução do Comitê Gestor da ICP-Brasil
DOC-ICP-nn.mm	Documento da ICP-Brasil vinculado ao DOC-ICP-nn	Instrução Normativa do ITI
ADE-ICP-nn.a	Adendo (formulário, modelo de documento, termo etc.) vinculado ao documento DOC-ICP-nn	Memorando do ITI
ADE-ICP-nn.mm.a	Adendo (formulário, modelo de documento, termo etc.) vinculado ao documento DOC-ICP-nn.mm	Memorando do ITI
MCT-xx-Vol. nn	Manual de Condutas Técnicas para os processos de homologação	Instrução Normativa do ITI

5.3.2 Normas ICP-Brasil

- **DOC-ICP-nn** – São os documentos principais, que trazem as diretrizes gerais sobre os diversos assuntos normatizados na ICP-Brasil. Sua criação e alteração depende sempre de aprovação do comitê gestor da ICP-Brasil, por meio de resoluções publicadas no Diário Oficial da União. Após a publicação, tanto da resolução quanto o texto do DOC-ICP-nn são divulgados em área especifica no sitio Web do ITI.
- **DOC-ICP-nn.mm** – São os documentos acessórios, destinados a suplementar, quando necessário, os DOC-ICP-nn. São aprovados por meio de instruções normativas do Instituto de Tecnologia da Informação (ITI), que recebeu essa competência do comitê gestor da ICP-Brasil conforme resolução n 33, de 21 de outubro de 2004, publicadas no Diário Oficial da União. Após a publicação, tanto a instrução normativa quanto o texto do DOC-ICP-nn.mm são divulgados em área especifica no sitio Web do ITI.

- **ADE-ICP-nn.aa** – São adendos derivados do DOC-ICP-nn: formulários, modelos e outros elementos que podem necessitar de alterações mais frequentes, sem prejuízo ao conteúdo das normas; por isso foram apartados do corpo dos demais documentos. Sua forma de aprovação e através de memorandos, e posterior divulgação no sitio Web do ITI.

- **ADE-ICP-nn.mm.aa** – São adendos derivados do DOC-ICP-nn.mm: formulários, modelos e outros elementos que podem necessitar de alterações mais frequentes, sem prejuízo ao conteúdo das normas; por isso foram apartados do corpo dos demais documentos. Sua forma de aprovação e através de memorandos, e posterior divulgação no sitio Web do ITI.

- **MCT-xx – Vol. nn** – Manuais de condutas Técnicas, que detalham os requisitos, materiais e testes necessários para homologação do produto âmbito da ICP-Brasil, são aprovados, também, por instruções Normativas do ITI, publicadas no Diário Oficial da União.

5.4 Declaração de Pratica de Certificação

Segundo Délio Silva Nunes (2007): Na Declaração de Práticas de Certificação (DPC) é especificado detalhadamente como que cada componente de uma ICP implementa a política de certificação. A DPC declara a PC associada e especifica os mecanismos e procedimentos utilizados para alcançar as políticas de segurança.

5.5 Política de Certificação

Segundo Délio Silva Nunes (2007): As PCs descrevem o papel de cada componente dentro da ICP, as responsabilidades assumidas pelos seus usuários para a requisição e uso dos certificados digitais, além da manutenção do par de chaves de responsabilidade dos usuários. As políticas de certificação devem abranger desde a solicitação do certificado, até a sua expiração ou revogação. As políticas de certificação não declaram os detalhes operacionais, pois estes podem ser alterados ao longo do tempo.

5.6 Auditoria

5.6.1 Auditoria Pré Operacional da Autoridade Certificadora

Segundo Délio Silva Nunes (2007): Auditoria pré-operacional de Autoridade Certificadora, todos os itens de segurança e procedimentos constantes das Resoluções, PC, DPC e PS da Autoridade Certificadora são considerados obrigatórios e têm seu cumprimento verificado durante a auditoria.

5.6.2 Auditoria Operacional de Autoridade Certificadora

Segundo Délio Silva Nunes (2007): Na auditoria operacional de AC verificam-se os mesmos itens que na pré-operacional, com a particularidade de que já existem registros de eventos realizados: certificados emitidos, revogados, logs dos acessos aos ambientes físico e lógico etc. Assim, através da análise de tais registros, pode-se avaliar se a AC está realizando adequadamente os procedimentos previstos.

5.6.3 Auditoria Pré Operacional da Autoridade de Registro

Segundo Délio Silva Nunes (2007): Auditorias pré-operacionais em Autoridades de Registro também abrangem as áreas de Segurança Física, Lógica, de Rede e de Pessoal, bem como Segurança da Informação e Ciclo de Vida dos Certificados.

5.6.4 Auditoria de Autoridade de Registro

Segundo Délio Silva Nunes (2007): A auditoria operacional de AR, além dos aspectos verificados na pré-operacional, enfatiza a análise dos certificados emitidos, buscando evidenciar a qualidade dos processos de identificação e validação dos solicitantes de certificados. A lista dos certificados emitidos pela AR, fornecida à auditoria pela AC responsável, é confrontada com os documentos de identificação e outros termos que devem estar armazenados pelos agentes de registro no ambiente da AR.

5.7 ICP-Brasil em Relação ao Mundo

Qualquer pessoa, órgão ou empresa pode criar sua própria cadeia de certificação. Existem sistemas pagos ou gratuitos, que podem ser buscados na Internet, com alto nível de sofisticação. A própria MP 2.200-2 não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento. Uma cadeia de certificação, entretanto, para ser amplamente aceita, precisa oferecer diversas garantias aos titulares e usuários de certificados.

5.7.1 Pontos que destacam a ICP-Brasil

- O par de chaves criptográficas deve ser gerado sempre pelo próprio titular e sua chave privada de assinatura é de seu exclusivo controle, uso e conhecimento.
- Os documentos assinados com processo de certificação da ICP- Brasil possuem presunção de validade jurídica.
- São utilizados padrões internacionais para os certificados bem como algoritmos criptográficos e tamanhos de chaves que oferecem nível de segurança aceitável internacionalmente
- As instalações e procedimentos das entidades credenciadas possuem nível de segurança física, lógica, de pessoal e procedimental em padrões internacionais;
- As entidades componentes da ICP-Brasil são obrigadas a declarar em repositório público as práticas de segurança utilizadas em todos os seus processos.
- As entidades estão sujeitas a auditoria prévia ao credenciamento e anualmente, para manter-se credenciadas.
- Os dados relativos aos certificados são mantidos por no mínimo 30 anos, para permitir comprovação e dirimir dúvidas sobre a assinatura de documentos, atendendo legislações específicas de guarda de documentos.
- Todas as AC são obrigadas a contratar seguro para cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco.
- É obrigatória a validação presencial dos titulares para obtenção de certificados.

6 Assinatura Digital

Como a assinatura em papel, trata-se de um mecanismo que identifica o remetente de uma mensagem eletrônica. Para a ICP-Brasil, a assinatura digital possui autenticidade, integridade, confiabilidade e o não-repúdio, seu autor não poderá, por forças tecnológicas e legais, negar que seja o responsável por seu conteúdo. A assinatura digital fica vinculada ao documento eletrônico que, caso seja feita qualquer alteração no documento, a assinatura se torna inválida. A técnica permite não só verificar a autoria do documento, como estabelece também uma “imutabilidade lógica” de seu conteúdo, pois qualquer alteração do documento, como por exemplo a inserção de mais um espaço entre duas palavras, invalida a assinatura.

Segundo William Stallings (2014): O *Nacional Institue of Standards and Tecnology* (NIST) publicou o *Federal Information Processing Standard* (FIPS 186), conhecido como algoritmo de assinatura digital (*Digital Signature Algorithm* – DSA). O DSA utiliza o *Secure Hash Algorithm* (SHA). O DSA foi proposto originalmente em 1991 e revisado em 1993 em resposta ao *feedback* público com relação à segurança do esquema. Houve outra revisão secundária em 1996. Em 2000, uma versão expandida do padrão foi emitida como FIPS 186-2. Essa versão mais recente também incorpora os algoritmos de assinatura digital baseados no RSA e na criptografia de curva elíptica.
O DSA utiliza um algoritmo que é projetado para oferecer apenas a função de assinatura digital. Diferente do RSA, ele não pode ser usado para a encriptação ou troca de chave. Apesar disso, esse é uma técnica de chave pública.

Segundo a Cert.br (2012): A assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada. A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isto. A verificação da assinatura e feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave publica correspondente pode decodifica-lo. A seguir será apresentando um método que traz mais segurança quanto ao uso das transações eletrônicas que os banco oferecem ao cliente (usuário).

7 Solução proposta

Como dito anteriormente, hoje os bancos oferecem diversos tipos de serviços por meio eletrônico seja ele um computador pessoal, notebook ou smartphone trazendo facilidade nas operações bancárias do cliente (usuário), a seguir será aprensentado uma técnica que traz mais segurança quanto a essas operações, garantindo que o usuário está de fato realizando tal operação eletrônica.

7.1 Transação Eletrônica Assinada Digitalmente

Muita das fraudes descritas acima poderiam ser evitadas com a aplicação do certificado digital para identificar toda e qualquer transação bancaria executada. A instituição financeira juntamente com uma AC (Autoridade Certificadora) como terceira parte da transação, disponibilizaria um certificado digital para seu cliente assinar e autorizar todas as transações em seu nome.

7.2 Login (Autenticação)

No momento de acessar o banco se solicita o certificado digital do cliente para que o mesmo se autentique no internet banking.

7.3 Transação Eletrônica

Toda e qualquer transação do cliente, o serviço do internet banking solicita a autenticação do cliente através de assinatura digital, garantindo que toda ação realizada seja feita pelo cliente identificado no certificado. O certificado digital assim substitui a necessidade do cliente de ficar informando os seus dados na página do internet banking, essas informações estão contidas no certificado digital, que por sua vez esta armazenado em uma mídia criptográfica com a senha do cliente.

8 Conclusão

Hoje temos acesso a internet por diversas formas, computador pessoal, notebook ou smartphone. Todas esses meios trazem facilidade para acesso a diversos serviços como redes sociais, mídas digitais, comércio eletrônico e acesso ao banco. Com isso estamos expondo informações particulares como endereço, número de documentos pessoais, senhas entre outras informações sensíveis. O roubo dessas informações está onde menos podemos prever e ficamos vulneráveis a ataques cibernéticos, roubo de informação e bens digitais.

Neste trabalho vimos as principais técnicas de crime cibernético e as fraudes cibernéticas utilizadas, o conceito de criptografia e suas principais caracteristicas, o uso do certificado digital e suas principais caracteristicas, quais são as principais informações que ele tem o os meios em que ele é disponibilizado e armazenado. Um breve conhecimento sobre infraestrutura de chaves públicas como, conceito e suas caracteristicas. A ICP-Brasil como PKI no Brasil, coordenada pelo Comitê Gestor as legislações que são necessarias para aderir a sua cadeia, as sua função quanto a regulamentação e auditoria da cadeia. Baseado nos conceitos apresentados, foi demonstrado uma técnica que pode mitigar a fraude eletrônica quanto ao uso do Internet Baking, tornando toda transação eletrônica assinada digitalmente.

Referências Bibliográficas e Internet

Edward,Fábio e Rodolfo; Criptografia em Software e Hardware, 2005, 288p.

William Stallings; Criptografia e Segurança de Rede de Computadores Princípios e Práticas, 2014, 558p.

Emilio T. N., Paulo L. de G.; Segurança de Redes em Ambientes Cooperativos, 2010, 483p.

Hugo Eiji Tibana Carvalho. Diponível em: http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2008_2/hugo/

Symantec. Disponível em: http://br.norton.com/cybercrime-definition. **Acesso em: 26 de Junho de 2016.**

Santander. Disponível em: https://www.santander.com.br/br/o-santander/seguranca/fraudes. **Acesso em: 26 de Junho de 2016.**

Cert.br. Disponível em: http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. **Acesso em: 26 de Junho de 2016.**

Instituto de Tecnologia da Informação. Disponível em: http://www.iti.gov.br/certificacao-digital/certificado-digital. **Acesso em: 26 de Junho de 2016.**

Globalsign. Disponível em: https://www.globalsign.com/pt-br/ssl-information-center/what-is-ssl/. **Acesso em: 26 de Junho de 2016.**

Globalsign. Disponível em: https://www.globalsign.com/pt-br/ssl-information-center/types-of-ssl-certificate/. **Acesso em: 26 de Junho de 2016.**

CriptoID. Disponível em: https://cryptoid.com.br/banco-de-noticias/carimbo-do-tempo/. **Acesso em: 26 de Junho de 2016.**

Criado por Délio Silva Nunes. Disponível em: http://www.gta.ufrj.br/grad/07_2/delio/index.html. **Acesso em: 27 de Junho de 2016.**