A Importância da Certificação Digital: Um Estudo Comparativo entre a Infraestrutura de Chaves Públicas Brasileira e a *Federal Public Key Infrastructure*

Rodrigo Gomes Tulha[1]
Professor-Orientador: Mario Teixeira Lemes[2]

RESUMO

As mudanças tecnológicas fomentadas pelo governo brasileiro, após a criação da Infraestrutura de Chaves Públicas Brasileira, tais como a adoção da nota fiscal eletrônica, permitiu a migração de serviços para a Internet, estes que somente poderiam ser realizados com a presença física para comprovação de autoria. Essa transição exige investimentos tecnológicos, adequações dos órgãos governamentais e esforços no sentido de compreender a real necessidade, os benefícios e as vantagens inerentes do uso dessas novas tecnologias, tais como a de certificação digital. O objetivo deste artigo é abordar o conceito, o funcionamento e a importância dos certificados digitais e das Autoridades Certificadoras responsáveis por emiti-los e gerenciá-los, bem como apresentar um estudo comparativo entre as principais infraestruturas emissoras de tais certificados no Brasil e no Estados Unidos.

Palavras-chave: Autoridade Certificadora. Certificado Digital. Criptografia.

ABSTRACT

Technological changes promoted by the Brazilian government after the creation of the Brazilian Public Key Infrastructure, such as the adoption of electronic invoicing, allowed the migration of services to the Internet, these that could only be performed with the physical presence for proof of authorship. This transition requires technology investments, adjustments of government agencies and efforts to understand the real need, the benefits and the inherent advantages of using these new technologies, such as digital certification. The purpose of this article is to discuss the concept, the operation and the importance of digital certificates and certification authorities responsible for sending them and manage them, and present a comparative study of major infrastructure issuing such certificates in Brazil and the United States.

Key-words: Certificate Authority. Digital Certificate. Encryption.

[1] Pós-graduando do curso Segurança em Redes de Computadores pela Faculdade de Tecnologia SENAI de Desenvolvimento Gerencial (FATESG). rodrigo@tulha.eng.br.

[2] Mestre em Ciência da Computação pela Universidade Federal de Goiás (UFG). mario.lemes@ifg.edu.br.

1. INTRODUÇÃO

O uso de certificados digitais está se popularizando no Brasil. Em 2010, segundo o Instituto Nacional de Tecnologia da Informação (ITI), a quantidade estimada para aquele ano era de 1,5 milhões. Um crescimento de 384% em relação ao ano de 2009 para certificados emitidos pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) (Lemes, 2011). Um levantamento publicado em janeiro de 2015 mostra que, entre dezembro de 2013 e dezembro de 2014, foram emitidos mais de dois milhões e meio de certificados. (http://www.iti.gov.br/images/icp-brasil/estrutura/2015/001_janeiro/TOTAL_DE_CERTIFICADOS_EM_2013_2014_Dez.pdf, 10/02/2015).

Outro fator decisivo para a popularização é o uso dos certificados digitais como tecnologia de autenticação, isso sem considerar o uso de *tokens* e *smartcards*, que são equipamentos de autenticação que também utilizam certificados.

Os *tokens* são amplamente usados por diversos seguimentos. Um exemplo de sua utilização é em sistemas bancários e sistemas jurídicos. Em relação a sistemas jurídicos, os *tokens* permitem o protocolo eletrônico de petições e o acesso a alguns serviços de cartórios, tais como o registro civil e o registro de imóveis.

Esse crescimento é um fator impulsionado, principalmente, por iniciativas do Governo Federal, através da Receita Federal do Brasil, como o uso de notas fiscais eletrônicas e a futura distribuição de certificados digitais para pessoas físicas, que será conhecido como o novo Registro de Identidade Civil (RIC). Através do RIC será possível identificar e legitimar pessoas físicas no âmbito da Internet. (http://acraiz.iti.gov.br/167-programas/identidade-digital-ric/117-identidade-digital-ric, 20/01/2015).

Outro projeto inovador do Governo Federal, sancionado pela Lei n° 12.933/2013, trata sobre a utilização de certificados digitais na carteira estudantil, o que possibilitará um controle mais efetivo e seguro sobre a emissão deste benefício (http://www.iti.gov.br/noticias/indice-de-noticias/4572-carteira-estudantil-utilizara-certificacao-icp-brasil, 21/01/2015).

Para acompanhar esse processo natural de evolução tecnológico do país, o governo instituiu a ICP-Brasil, uma combinação de *softwares*, tecnologias de

encriptação e serviços, o que permitiu melhorar e agilizar as comunicações e negócios realizados pela Internet entre pessoas, empresas e órgãos públicos.

De acordo com Stallings (2007, p 289) “Uma Infraestrutura de Chave Pública é definida como um conjunto de *hardware*, *software*, pessoas e procedimentos para criar, gerenciar, armazenar, distribuir e revogar certificados digitais.”

A assinatura digital é uma das tecnologias constituintes da ICP-Brasil. Pode-se definir assinatura digital como um mecanismo de autenticação que permite o criador de uma mensagem anexar um código que atue como uma assinatura, o que garante a origem e a integridade da mensagem enviada. (Lemes, 2011)

A ideia da assinatura digital é a mesma de uma assinatura feita a mão. A assinatura feita a próprio punho é um ato que garante a verdadeira identidade do requisitante da informação ou do serviço. Como garantir isso através da Internet? Para atingir esse requisito, a ICP-Brasil adota o uso de certificados digitais.

Os certificados substituem o modo tradicional de assinatura que exige a presença física para garantir a veracidade da mesma. Os papéis, no formato digital, geram flexibilidade, redução de custos, acesso rápido a informação e economia de tempo.

Uma AC é uma entidade pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. (http://www.iti.gov.br/certificacao-digital/autoridades-certificadoras, 13/11/2014).

Em 24 de agosto de 2001, por meio de medida provisória (MP) n° 2.200-2, o Instituto Nacional de Tecnologia da Informação (ITI) foi transformado em autarquia e na Autoridade Certificadora Raiz (AC-Raiz), o que possibilitou a criação efetiva da ICP-Brasil. O governo brasileiro deu legitimidade à ICP-Brasil, tornando possível identificar e confiar em uma entidade qualquer, seja ela uma pessoa, uma estação de trabalho ou outra forma de entidade eletrônica.

O objetivo deste trabalho é realizar um estudo comparativo entre a ICP-Brasil e a *Federal Public Key Infrastructure* (FPKI). Para atingir o objetivo, há a necessidade de Ilustrar e descrever o funcionamento da estrutura de cada uma das infraestruturas e realizar o levantamento e a análise das principais características, algoritmos e funções criptográficas, e requisitos relacionados com a segurança e a privacidade da informação.

Este trabalho está dividido da seguinte forma. A Seção 2 abrangerá conceitos gerais das duas estruturas. Na Seção 3 tratará sobre a ICP-Brasil, sua estrutura e elementos que compõem a mesma. Na Seção 4, da mesma forma que a Seção anterior, tem-se a apresentação da FPKI, sua estrutura e os elementos que a compõem. A Seção 5 é responsável por apresentar os resultados deste trabalho, um estudo comparativo entre a ICP-Brasil e a FPKI. Finalmente, na Seção 6, tem-se a conclusão, a definição e a direção de trabalhos futuros.

2. CONCEITOS GERAIS

A assinatura digital é um mecanismo que anexa um código na mensagem ou documento para ser transmitido. Esse mecanismo garante:

- Veracidade do emissor;
- Não repúdio;
- Imutabilidade do conteúdo pelo receptor.

O código anexo é formado por um *hash* e é criptografado com a chave privada do transmissor. A função de assinatura é a primeira ser aplicada, através da criação do *hash,* e posteriormente é realizada a função de confidencialidade, através da criptografia. A figura 2 ilustra a o funcionamento da assinatura digital com a utilização da função *hash* e de um algoritmo criptográfico.

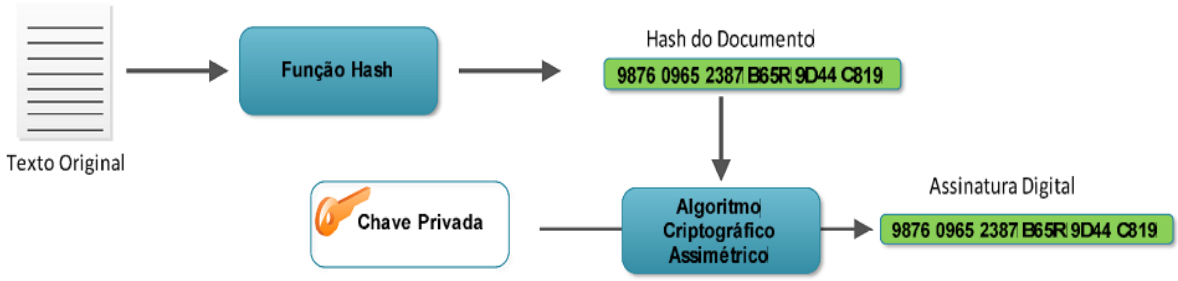

Figura 2 - Criptografia e função hash.

Segundo Stallings (2007, p. 274) a assinatura digital pode ser dividida em duas categorias: direta ou arbitrada. O método direto envolve apenas as partes em comunicação: a origem e o destino. Nesse método considera-se que o destino

conhece a chave pública da origem. Assim, a criptografia é realizada com a chave privada do emissor.

A fragilidade do método de assinatura digital direta está na transmissão da chave pública ao receptor que pode ser interceptada ou ainda o emissor poder negar o envio da mensagem, alegando que a chave privada foi perdida ou roubada.

No método arbitrado, existe uma terceira parte confiável, chamado de árbitro, as chamadas AC's, o que garante a autenticidade do emissor, ou seja, é assegurado que a assinatura não será falsificada e que o emissor não negará a assinatura.

A criptografia assimétrica é a distribuição da uma chave pública, que será conhecidas por todos, e outra a chave privada que é secreta. Quando uma entidade envia uma mensagem para outra, é feito a criptografia com a chave pública e somente o dono da chave privada pode abrir a mensagem. A figura 3 ilustra a chave pública e privada da criptografia assimétrica (Stallings, 2007, p. 183).

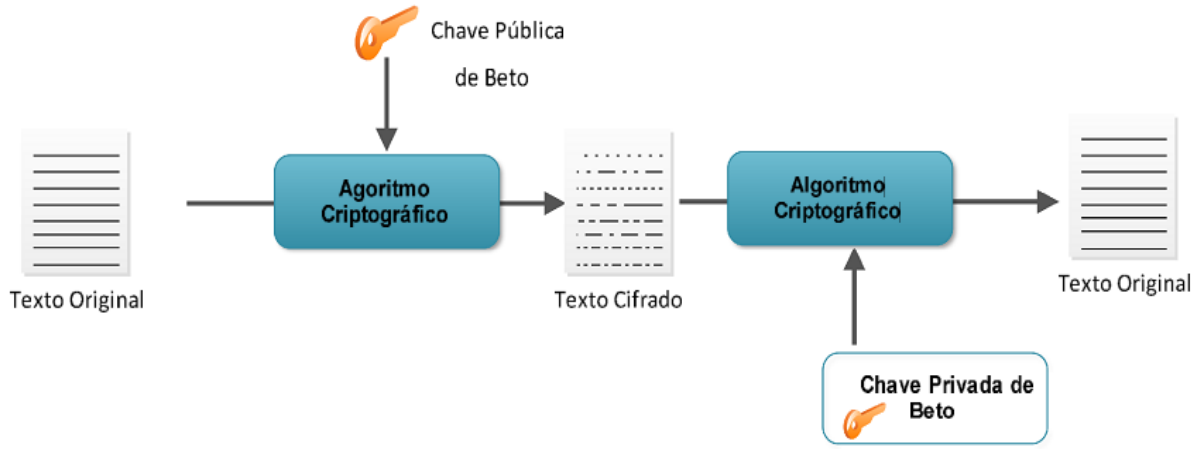

Figura 3 – Chaves pública e privada da criptografia assimétrica.

Os certificados digitais são formados por chaves públicas e privada relacionadas a alguma pessoa/entidade assinadas por uma entidade confiável, uma Autoridade Certificadora (AC).

Os certificados digitais emitidos pelas AC's são implementados no formato do padrão X.509 v3 que define uma estrutura de abastecimento de serviços de autenticação pelo diretório X.500 aos seus usuários. São organizados pelo protocolo *Lightweight Directory Access Protocol* v3 (LDAP v3) (Silva, 2004, p. 213) de serviços

de diretório, que juntos tem a função de organizar hierarquicamente toda a ICP e prover o serviço de autenticação.

3. INFRAESTRUTURA DE CHAVES PUBLICA BRASILEIRA

Esta Seção é responsável por realizar o estudo sobre a estrutura da ICP-Brasil e dos elementos e protocolos criptográficos que a compõem.

3.1. ESTRUTURA DA ICP-BRASIL

A ICP-Brasil é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual. (http://www.iti.gov.br/index.php/icp-brasil/o-que-e , 01/10/2014).

A AC-Raiz é a primeira autoridade da cadeia de certificação, ela executa as políticas de certificados e normas técnicas e operacionais aprovados pelo Comitê Gestor da ICP-Brasil. Portanto, compete a AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das AC's de nível imediatamente subsequente.

Além de realizar auditoria e fiscalizar as AC's, as Autoridades de Registros (AR), as Autoridades de Carimbo de Tempo (ACT) e demais Prestadoras de Serviço de Suporte (PSS) habilitadas, também têm a responsabilidade de emitir a Lista de Certificados Revogados (LCR). (http://www.iti.gov.br/icp-brasil/estrutura, 17/12/2014).

As AC's possuem responsabilidades e funções idênticas a AC-Raiz. As AC's emitem, distribuem, renovam, revogam e gerenciam os seus certificados mas não possuem poderes de fiscalização sob as entidades subsequentes da hierarquia. As AC's são classificadas por níveis, as que estão logo abaixo a AC-Raiz são de nível 1, logo abaixo de nível 2 e assim sucessivamente. Em relação as AC's de nível 1, podem-se citar:

- Serpro;
- Serasa;
- Soluti;
- Certisign;
- Receita Federal.

As AR's são entidades que também têm contato direto com os usuários finais, como as AC's. Elas fazem o intermédio entre os usuários e as AC's logo acima na hierarquia. As AR's são responsáveis pelo recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, dos solicitantes.

Devido ao modelo hierárquico adotado no Brasil não é possível a AC-Raiz emitir um certificado diretamente ao um usuário final, mas todos os procedimentos realizados nas AR's podem ser feitos nas AC's. Uma AR é reconhecida pela AC por meio de um nome e pela sua chave pública, mediante a conferência da assinatura da AR em uma mensagem.

A partir de 2013, uma nova entidade foi inserida na ICP-Brasil, a ACT, que é uma entidade confiável de tempo que tem por responsabilidade emitir carimbos de tempo que, associado a uma assinatura digital, concede provas da sua existência em um determinado período, em qualquer documento ou transação eletrônica. Note na figura 1 o funcionamento de uma ACT.

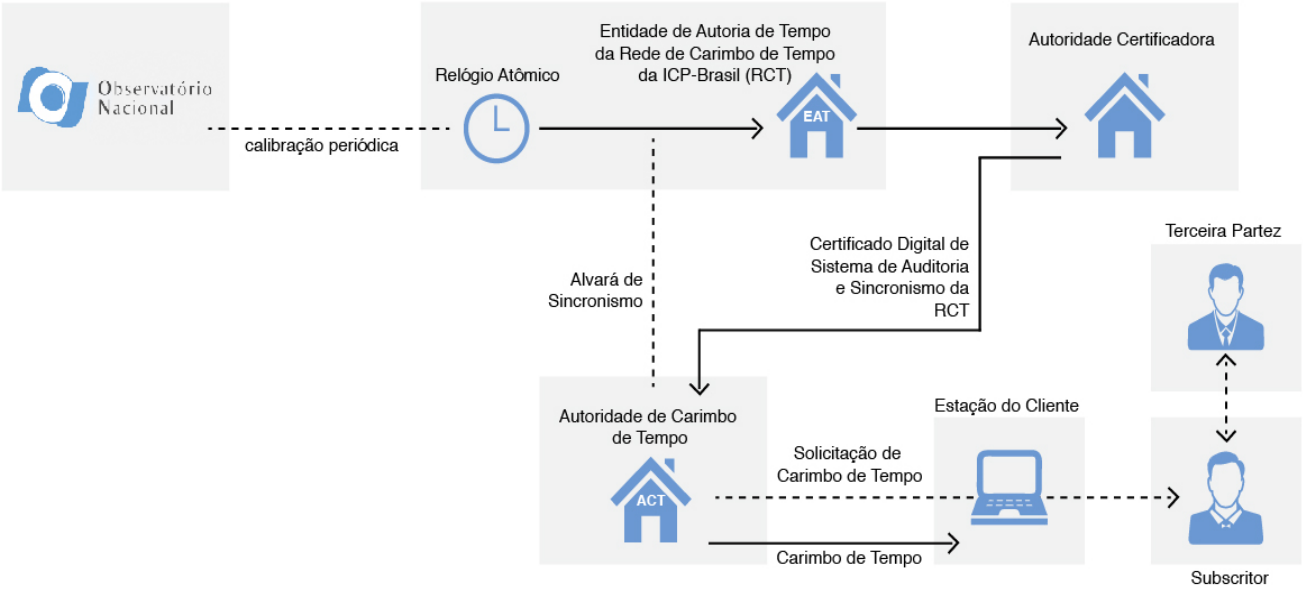

Figura 1 - Funcionamento de uma ACT.

Os certificados emitidos são válidos por um período estipulado pela AC. Após esse tempo, os mesmos são colocados na LCR, o que não inviabiliza a invalidação ou a revogação destes certificados antes do tempo pré-determinado.

As razões para uma revogação do certificado variam, como a modificação dos atributos do proprietário, que podem ser mudança de *e-mail*, dos dados da empresa, do nome ou de outro qualquer campo do certificado.

Outra razão para a revogação de um certificado pode ser o comprometimento da chave privada de uma das entidades, seja por roubo, perda, modificação ou acesso indevido, o que torna a relação entre as entidades não mais confiável.

A revogação de um certificado somente pode ser feito pelo proprietário do mesmo ou pela AC emissora. Já a disponibilização desta informação é responsabilidade da AC, através da LCR.

3.2. ELEMENTOS ESTRUTURAIS E RESPONSABILIDADES DOS PARTICIPANTES DA ICP-BRASIL

A estrutura da ICP-Brasil é formada por um Comitê Gestor (CG), uma AC-Raiz, as AC's, AR's e ACT's. Outra entidade participante são as PSS, porém as mesmas não estão representadas na estrutura da ICP-Brasil.

Dentre as obrigações das AC's dentro da estrutura da ICP-Brasil, podem-se citar:

- Adoção de medidas de segurança e controle;
- Manutenção da conformidade dos seus processos, procedimentos e atividades, de acordo com as normas práticas e regras;
- Manutenção e garantia da integridade, sigilo e segurança da informação.
- Processos de testes regulares sobre seu Plano de Continuidade de Negócio;
- Disponibilização de informação as terceiras partes e aos titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro.

A arquitetura adotada pela ICP-Brasil é a de certificação com raiz única ou hierárquico, sendo o ITI, a AC-Raiz. Esse modelo também é idêntico aos da

Alemanha, da Coréia do Sul, da Índia, da Austrália, do México e Japão (Silva, 2004, p. 237). A figura 4 ilustra o modelo de raiz única ou hierárquico.

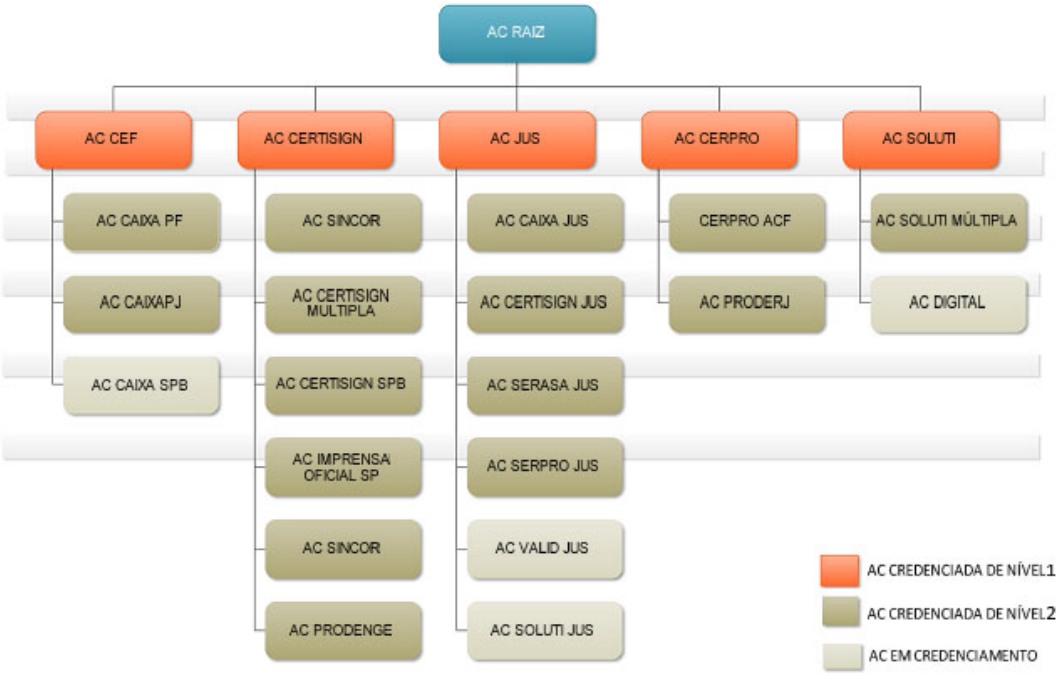

Figura 4 – Modelo de Hierarquia de Raiz Única.

O CG da ICP-Brasil é a entidade máxima, responsável pelo estabelecimento e pela administração das políticas a serem seguidas pelas AC's integrantes do governo e do setor privado, sendo assessorado pelo Comitê Técnico. De acordo com a MP n° 2.200-2 o CG possui inúmeras responsabilidades. Algumas delas são:

- Adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;
- Estabelecer a política de cerificação e as regras operacionais da AC-Raiz;
- Homologar, auditar e fiscalizar a AC-Raiz e seus prestadores de serviço;
- Estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC's e das AR's e definir níveis da cadeia de certificação;
- Aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC's e AR's, bem como autorizar as AC-Raiz a emitir certificados;

- Atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-brasil.

A figura 5 demonstra a hierarquia da estrutura da ICP-Brasil.

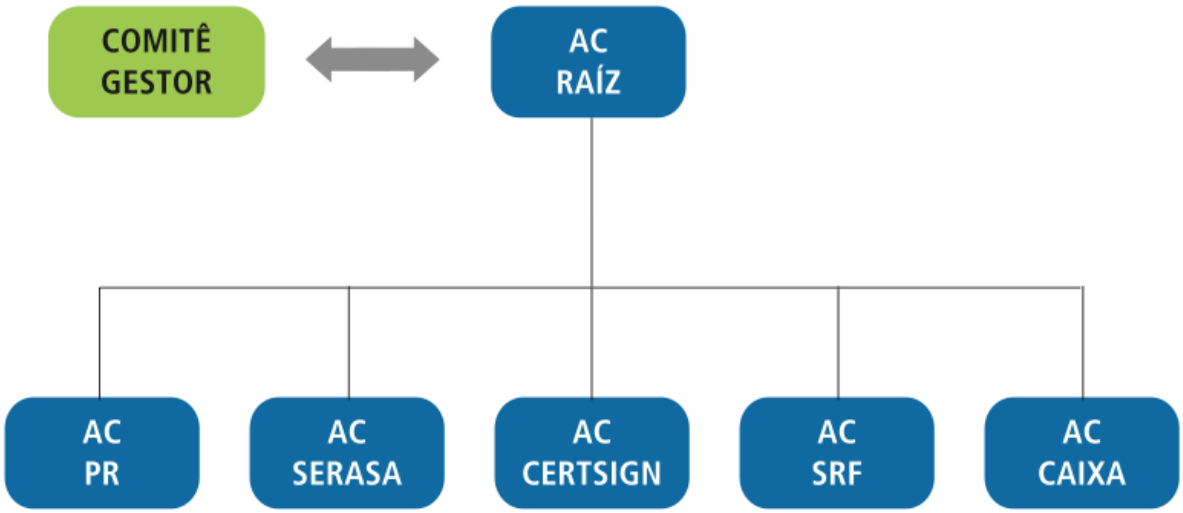

Figura 5 – Estrutura hierárquica da ICP-Brasil.

O CG mantém uma documentação desde a criação da ICP-Brasil. Estes documentos compõe a estrutura normativa da ICP-Brasil, os quais são:

- DOC-ICP-nn: são os documentos principais, que trazem diretrizes gerais sobre assuntos normatizados. As dua letras “nn” são números que identificam o documento;
- DOC-ICP-nn.mm: são documentos acessórios, que suplementam os documentos principais;
- ADE-ICP-nn.aa: identificam adendos derivados do DOC-ICP-nn, são formulários, modelos e outros elementos que podem exigir alterações frequentes;
- ADE-ICP-nn.mm.aa: são adendos derivados do DOC-ICP-nn.mm, também podem ser formulários, modelos e outros elementos;
- MCT-xx – Vol. nn: são manuais de conduta técnicas, que detalham os requisitos, materiais e teste necessários para homologação de produtos no âmbito da ICP-Brasil.

O DOC-ICP e MCT-xx são aprovados por meio de instrução normativa e o ADE-ICP é através de memorando (Silva, 2004, p. 281).

Os documentos definem e normatizam questões sobre quais protocolos utilizar, além de orientar sobre as políticas de segurança que devem ser seguidas por todas as entidades integrantes da ICP-Brasil. Outras orientações são acerca das práticas de certificação, sobre o credenciamento e atribuições das entidades, entre outras aplicações (Silva, 2004, p. 281).

Os custos para implantação de uma AC são altos, estima-se que cerca de R$ 1 milhão de reais (Silva, 2004, p. 250). Dentre as várias taxas cobradas, fizemos um levantamento informal junto a uma AC de nível e obtemos alguns valores pagos em 2014, os quais são:

- Taxa de credenciamento - R$ 500.000,00 pela AC de primeiro nível;
- Taxa de fiscalização - A auditoria realizada na AC de primeiro nível não tem custo pois é realizada pelo próprio ITI. As ACs de segundo nível utilizam auditores independentes e os valores variam entre R$ 25.000,00 e R$ 40.000,00 anuais dependendo da empresa contratada;
- Taxa de renovação da AC de primeiro nível R$ 100.000,00.

3.3. PRINCIPAIS PROTOCOLOS E FUNÇÕES CRIPTOGRÁFICAS

Os principais protocolos criptográficos utilizados para assinatura digital no Brasil seguem as orientações do *National Institute of Standars and Tecnology* (NIST) que publica constantemente notas sobre estudos, testes, provas de conceitos dos protocolos atualmente utilizados, informando sobre possíveis fragilidades e falhas de segurança.

O protocolo criptográfico recomendado pelo NIST, o Rivest-Shamir-Adleman (RSA) (Stallings, 2007, p. 181), é uma cifra de bloco em que o texto claro e texto cifrado são inteiros entre 0 e n – 1 para algum n, calculado exponencialmente (Stallings, 2007, p. 189).

Para a função *hash* utiliza o algoritmo *Secure Hash Algorithm* (SHA) (Stallings, 2007, p. 253), desenvolvido pelo próprio NIST, o qual processa entradas em blocos anexando *bits* de complementação e possui chaves de tamanho menor que 256 *bits*.

O novo padrão SHA-2 é mais robusto devido ao tamanho das chaves que que estão entre 256 e 512 *bits* (Stallings, 2007, p. 253). Para geração das chaves assimétricas é utilizado o algoritmo *Elliptic Curve Cryptography Brainpool* (ECC *Brainpool*) (https://tools.ietf.org/html/rfc5639, 20/01/2015), que através de cálculos de curvas elípticas finitas geram códigos de criptografia.

Após a publicação do DOC ICP-01.01 **(** < http://www.iti.gov.br/images/legislacao/Docicp/DOC-ICP-01.01_-_versao_2.5_PADROES_E_ALGORITMOS_CRIPTOGRAFICOS_DA_ICP-BRASIL.pdf , 2014**)**pela ICP Brasil, em meados de junho de 2014, que trata sobre os novos padrões e algoritmos criptográficos, além de findar com os prazos publicados na resolução n°68, determinou-se o término de uso da função *hash* SHA-1 e os algoritmos criptográficos RSA 1024 e RSA 2048 para criação de certificados digitas. A partir desta data passou-se a vigorar a utilização do SHA-2 e RSA 4096.

A Tabela 1 apresenta os algoritmos e o tamanho das chaves usados pelas AC's da ICP-Brasil. Já na Tabela 2 tem-se os algoritmos e os tamanhos de chaves utilizados entre as entidades e os usuários finais.

Tabela 1 – Chaves Assimétricas das ACs.

Geração de Chaves Assimétricas de AC	
Algoritmo	RSA, ECC-brainpool512r1
Tamanho da Chave	RSA 2048, RSA 4096, brainpoolP512r1

Fonte: DOC-ICP-01.01

Tabela 2 – Chaves Assimétricas dos Usuário Final.

Geração de Chaves Assimétricas de Usuário Final	
Algoritmo	RSA, ECC-brainpool
Tamanho da Chave A1, A2, A3, S1, S2, S3, T3	RSA 1024, RSA 4096, brainpoolP256r1
Tamanho da Chave A4, S4, T4	RSA 1024, RSA 4096, brainpoolP512r1

Fonte: DOC-ICP-01.01

4. *FEDERAL PUBLIC KEY INFRASTRUCTURE*

Esta seção trata sobre a estrutura da FPKI, dos elementos que a compõem e dos principais protocolos e funções criptográficas utilizados pela mesma.

4.1. ESTRUTURA DA FPKI

A FPKI foi criada no ano de 2000. Esse nome foi dado para diferenciar de outras ICP's privadas que já existiam antes de sua criação. A FPKI foi idealizada pelo *Government Information Technology Services* (GITS), co-presidida pelo *Office of Management and Bugdet* (OMB) e pelo *National Partinership for Reinventing Government* (http://www.idmanagement.gov/sites/default/files/documents/pki-brochure.pdf,12/12/2014).

Atualmente a FPKI é composta pela *FPKI Management Authority* (FPKIMA) e opera com quatro AC's na seguinte estrutura de confiança: *Federal Bridge Certification Authority* (FBCA), *Federal Common Policy Certification Authority* (FCPCA), *E-Governance Certification Authority* (EGCA) e *Citizen and Commerce Class Common Certification Authority* (C4CA).

A FPKIMA é responsável por operar e manter as políticas padrões das AC's. A FBCA, como o próprio nome sugere, faz a ponte ou ligação ponto a ponto entre as ICP do Governo Federal dos EUA e outros domínios de entidades de ICP.

A FBCA gera certificados que forma uma estrutura de confiança em toda a FPKI. A FCPCA atua como a ancora de confiança para os domínios FPKI, emitindo certificados para a AC *Shared Service Provider* (SSP). A EGCA foi criada para garantir a autenticação e confiança mútua através de certificados, estabelecendo canais de comunicação seguros entre entidades reconhecidas e confiáveis.

Finalmente, a C4CA é um mecanismo para habilitar um domínio de confiança na ICP, satisfazendo o nível 2, com propósito de garantir a confiança entre ICP's comerciais. Note na figura 6 a estrutura hierárquica da FPKI.

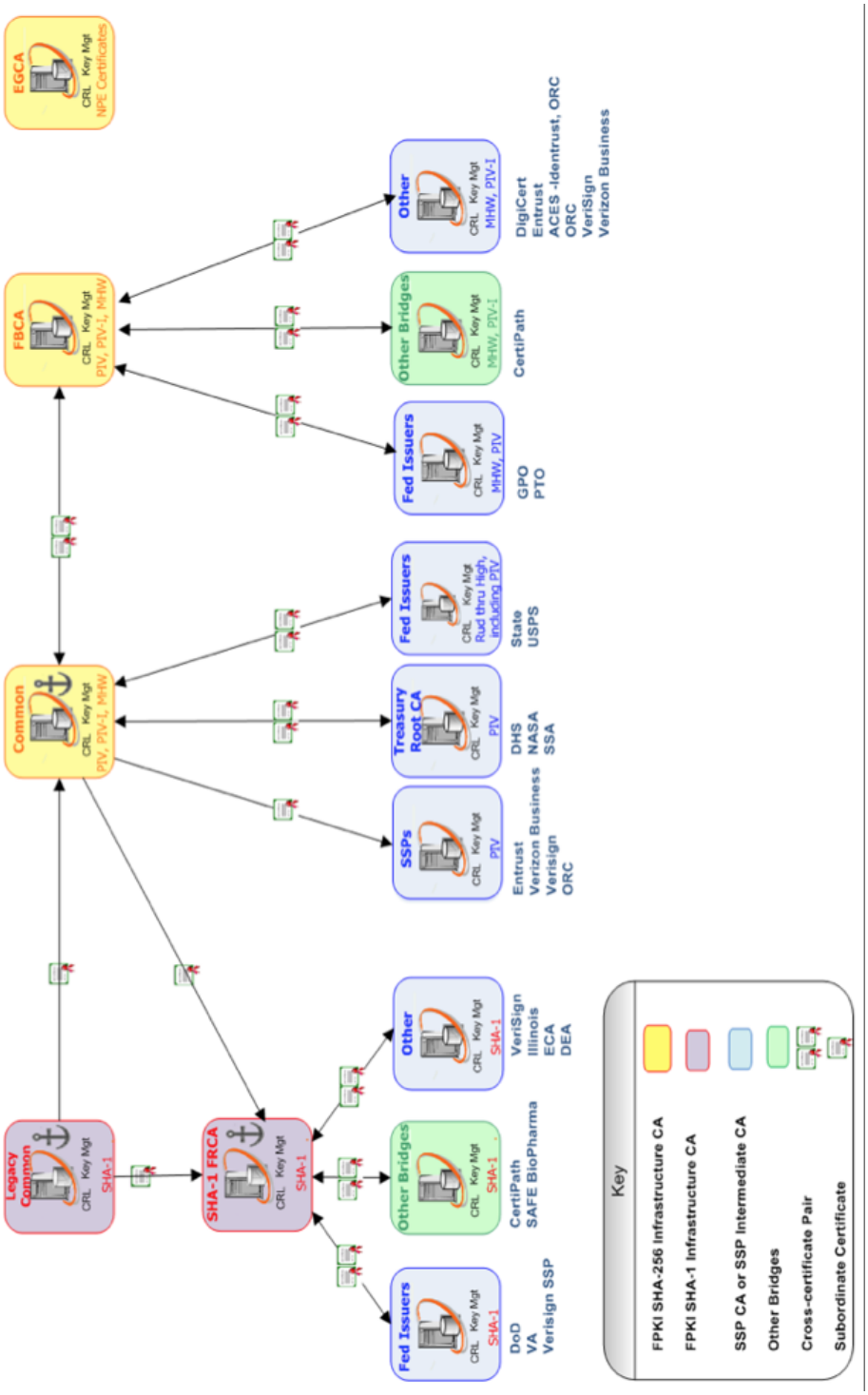

Figura 6 – Estrutura hierárquica da FPKI

4.2. ELEMENTOS ESTRUTURAIS DA FPKI

O principal órgão federal de administração e operação da estrutura da FPKI é o *Federal Chief Information Officers Council (Federal* CIO Council*)*. Esse órgão estabelece o *framework* de interoperabilidade da FPKI e supervisiona o

funcionamento das organizações responsáveis por governar e promover a sua utilização.

A *Federal PKI Policy Authority (*FPKIPA*)* é um grupo de agências do Governo Federal do U.S indicados pelo *Federal CIO Council*, e tem as seguintes responsabilidades:

- Manter a políticas de certificados;
- Implementar, fiscalizar e manter as políticas de certificados da FBCA;
- Comunicação de práticas de certificação da FBCA;
- Receber os pedidos de entidades que desejam interagir usando a FBCA;
- Garantir e fiscalizar que as AC's cumpram as políticas de certificados da FBCA, para manterem-se na estrutura de confiança.

Como visto anteriormente, a FBCA faz um ponte entre as entidades participantes da estrutura a arquitetura. Essa características é chamada de *mesh*, onde a principal AC pode ser qualquer AC designada pela entidade que está ligada ou tem uma relação de confiança com a FBCA. A figura 7 ilustra a relação de confiança entre as entidades e os usuários finais.

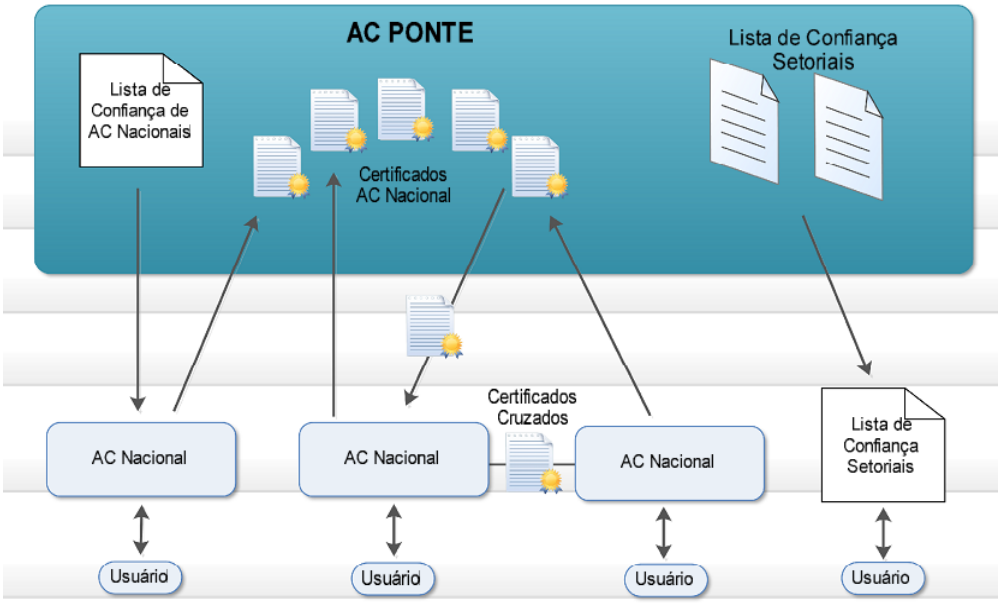

Figura 7 - Relação entre as entidades e os usuários finais.

O NIST é um instituto de tecnologia e padronização nos Estados Unidos, assim como o Inmetro no Brasil, e possui um divisão de segurança de computadores que, através das *Federal Information Processing Standards* (FIPS), promulga

normas e diretrizes de segurança de computadores, além de apresentar informações relevantes de apoio e pesquisa.

4.3. PRINCIPAIS PROTOCOLOS E FUNÇÕES CRIPTOGRÁFICAS

A FPKI segue as orientações do NIST, assim como a ICP-Brasil. Através das FIPS podem-se atualizar, corrigir e manter os protocolos e funções criptográficos utilizados.

A FIPS 180-4 (http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf, 10/02/2015) publicada em março de 2012, trata sobre a padronização do *hash* de segurança e especifica que o algoritmo para função *hash* que pode ser usado é o SHA-2.

Já a FIPS 186-4 (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf, 10/02/2015), publicada em julho de 2013, padroniza o algoritmo de criptografia da assinatura digital. Essa FIPS orienta que a utilização do algoritmo RSA com chave de tamanho de 3072 *bits* Em 2014, o NIST publicou um rascunho da FIPS 202, que tratará de um possível padronização para o uso do SHA-3.

5. UM ESTUDO COMPARATIVO ENTRE A ICP-BRASIL E A FPKI

De acordo com as características apresentadas as seções anteriores, foi possível a criação da Tabela 3, uma tabela que reúne as principais informações extraídas, e realizar um estudo comparativo sobre as principais hierarquias de certificação no Brasil e nos Estados Unidos: a ICP-Brasil e a FPKI. A coluna itens refere-se aos elementos de comparação selecionados e as outras duas colunas os tipos ou características para cada infraestrutura.

A primeira característica, a coluna “Ano de Criação, mostra o quanto o Brasil demorou para perceber da importância da criação de uma ICP. A estrutura e o funcionamento da ICP-Brasil é bastante burocrático. Outro característica notável é a dificuldade da criação ou adequação das leis ou de documentos gerados que normatizam a utilização.

Os protocolos criptográficos das ICP’s são diferentes, a ICP-Brasil atualizou-se mais rápido que a FPKI, utilizando um algoritmo mais complexo e resistentes a ataques, o RSA com 4096 *bits*.

A função *hash,* utilizada para resumo das mensagens, e o padrão dos certificados X.509 v3 são os mesmos em ambos. O principal fator dessa característica é a influência mundial do NIST.

Em relação ao modelo de raiz utilizado, a ICP-Brasil adota o modelo de raiz única, o que proporciona interoperabilidade e simples convergência com outras ICP's, pois a administração e organização está concentrada em uma única entidade.

A comunicação torna-se mais fácil e rápida de ser modificada dentro de toda a estrutura, seja a mudança de um padrão de criptografia, de uma função ou um algoritmo diferente das outas ICP's.

O modelo *mesh*, adotado pela FPKI, devido as inúmeras relações de confianças, requer que cada nó seja avisado sobre a diferença de padrões para que toda a estrutura se comunique de acordo com o padrão da outra ICP.

A privacidade da informação no modelo de raiz única pode ser comprometida pois é possível "bisbilhotar" as informações do certificado devido a concentração das informações geradas pela AC-Raiz. No modelo *mesh* não existe essa possível quebra de privacidade por não existir essa centralização e controle da AC-Raiz.

Um ponto negativo da ICP-Brasil é o órgão gestor ser uma instituição estatal. Essa característica torna todo o processo de funcionamento da ICP moroso e burocrático, e restringe todo a operação da ICP ao CG. Diferentemente da FPKI, a qual nota-se a existência de uma relação de confiança cruzada entre as entidades. Dessa forma, o certificado, além de não perder o sigilo, tem sua operação não restrita a nenhum órgão ou entidade.

Os dois modelos possuem algoritmos de criptografia seguros, o que garante a legitimidade do emissor e integridade da informação. Na ICP-Brasil, caso uma senha seja descoberta, uma informação seja alterada ou o roubo de uma chave seja efetuado, há o comprometimento de toda a estrutura devido a um possível atraso de anúncio e revogação deste certificado pela AC-Raiz.

A FPKI não sofre com a demora do anúncio de revogação. Uma vez revogado o certificado, a relação de confiança é desfeita com a AC que gerou o certificado e é invalidado pela mesma, sem a necessidade de anunciar por toda a ICP.

A iniciativa da ICP-Brasil de atualizar o protocolo de criptografia torna os certificados digitais e as comunicações entre as entidades mais segura, porém é

obscura em relação a possibilidade do principal órgão de administração ter acesso ao conteúdo do certificado digital, o que torna a infraestrutura nebulosa. Veja na Tabela 3 as principais características comparativas entre a ICP-Brasil e a FPKI.

Tabela 3 – Um estudo comparativo entre a ICP-Brasil e FPKI

Itens	ICP-Brasil	FPKI
Ano de Criação	2001	2000
Protocolos Criptográficos	RSA 2048, RSA 4096	RSA 2048, RSA 3072
Função *Hash*	SHA-2	SHA-2
Padrão do Certificado	X.509 v3	X.509 v3
Modelo	Hierárquico (AC-Raiz)	*Mesh* (Ponte, Confiança)
Confiança do Algoritmo	Seguro	Seguro
Interoperabilidade	Simples	Complexa
Falha de Segurança	Compromete toda estrutura	Compromete apenas uma relação
Privacidade do Certificado	Podem perder sigilo	Não perdem sigilo
Operação da AC	Restrita ao CG	Livre
Leis	Inconsistente	Consistentes
Crescimento da Estrutura	Lento	Rápido

6. CONCLUSÃO

O uso de certificação digital, com o objetivo de tornar operações ágeis, seguras e desburocratizadas, levou a popularização desta tecnologia e desde de 2011, de acordo com os levantamentos realizados, têm o crescimento alavancado a cada ano.

A utilização dos certificados digitais agilizam as comunicações e negócios realizados através da Internet. Os bancos, empresas e a população em geral utilizam os certificados para tornar o contato ou negociação entre as partes mais segura.

Com os levantamentos realizados conseguimos verificar o quanto toda ICP brasileira é mais lenta, mas mantém os algoritmos atualizados garantindo a segurança dos certificados contra possíveis fraudes.

Este artigo teve como objetivo a realização de um estudo comparativo entre a ICP-Brasil e a FPKI. Como objeto de análise, foram comparados os algoritmos de criptografias utilizados, as funções utilizadas para assinatura digital, os modelos de hierarquia, e alguns itens relacionados a privacidade e a segurança da informação, até mesmos relacionados às leis e operação de ambas infraestruturas.

Como trabalhos futuros pretende-se realizar um estudo sobre os algoritmos criptográficos utilizados pela ICP em todas as suas comunicações, seja ela entre AC e usuários finais, de AC para AC ou AC para AR, e verificar o nível de complexidade e forma de transmissão de cada um dos possíveis cenários.

7. REFERÊNCIA BIBLIOGRÁFICA

Emiliano S. M. e Maria H. M. **Certificados Digitais**: Conceitos e Práticas. São Paulo: Ed. Brasport, 2007.

ITI, Disponível em: < http://www.iti.gov.br/images/servicos/homologacao/MCT4_Vol.I.pdf >. Acesso em: 05 set. 2014.

ITI, Disponível em: <http://www.iti.gov.br/images/servicos/homologacao/MCT8_-_Vol.I.pdf>. Acesso em: 05 set. 2014.

ITI, Disponível em: < http://acraiz.iti.gov.br/167-programas/identidade-digital-ric/117-identidade-digital-ric >. Acesso em: 21/01/2015

ITI, Disponível em: < http://www.iti.gov.br/noticias/indice-de-noticias/4572-carteira-estudantil-utilizara-certificacao-icp-brasil >. Acesso em: 20/01/2015

ITI, Disponível em: < http://www.iti.gov.br/images/legislacao/Docicp/DOC-ICP-01.01_-_versao_2.5_PADROES_E_ALGORITMOS_CRIPTOGRAFICOS_DA_ICP-BRASIL.pdf >. Acesso em: 24/01/2014. Brasília, 2014.

ITI, Disponível em: < http://www.iti.gov.br/images/icp-brasil/estrutura/2015/001_janeiro/TOTAL_DE_CERTIFICADOS_EM_2013_2014_Dez.pdf >. Acesso em: 24/01/2014. Brasília, 2014.

Lemes, Mario Teixeira e Filho, Helio Ribeiro de Brito. **Implementação de uma Entidade Certificadora**. 2011. 109 f. Trabalho de Conclusão de Curso (Graduação Engenharia da Computação). Universidade Católica de Goiás, Goiânia, 2011.

NIST, Disponível em: < http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf >. Acessado em 10/02/2015.

NIST, Disponível em: < http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf >. Acessado em 10/02/2015.

NIST, Disponível em: < http://csrc.nist.gov/publications/drafts/fips-202/fips_202_draft.pdf >. Acessado em 10/02/2015.

Presidência da República Casa Civil. MP n° 2.200-2. Disponível em: < http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm >. Acesso em: 17/12/2014. Brasília, 2001.

Request for Comments. RFC5639: Elliptic Curve Cryptografy (ECC) Brainpool Standard Curves and Curve Generation Disponível em: < https://tools.ietf.org/html/rfc5639 >. Acesso em: 20/01/2015.

Silva, Ino Sarlo da. **Public Key Infrastructure** - Conheça a Infraestrutura de Chaves Públicas e a Certificação Digital. São Paulo: Novatec Editora, 2004.

Site do Governo Federal do E.U.A. Disponível em: < http://www.idmanagement.gov/federal-public-key-infrastructure > Acesso em: 12 dez. 2014.

Site do Governo Federal do E.U.A. Disponível em: < http://www.idmanagement.gov/sites/default/files/documents/pki-brochure.pdf > Acesso em: 12 dez. 2014.

William Stallings. **Criptografia e Segurança de Redes** – Princípios de Práticas, 4° Edição, Ed. Prentice Hall, 2007.