CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

Serviço de Assinatura Digital ICP-Brasil via *Web*

LEANDRO YUKIO MANO ALVES

Marília, 2013

CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

Serviço de Assinatura Digital ICP-Brasil via *Web*

Monografia apresentada ao Centro Universitário Eurípides de Marília como parte dos requisitos necessários para a obtenção do grau de Bacharel em Ciência da Computação.
Orientador: Prof. Dr. Fábio Dacêncio Pereira.

Marília, 2013

CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

TRABALHO DE CONCLUSÃO DE CURSO – AVALIAÇÃO FINAL

Leandro Yukio Mano Alves

Serviço de Assinatura Digital ICP-Brasil via Web

Banca examinadora da monografia apresentada ao Curso de Bacharelado em Ciência da Computação do UNIVEM/F.E.E.S.R., para obtenção do Título de Bacharel em Ciência da Computação.

Nota: 9,0 (nove)

Orientador: Fábio Dacêncio Pereira

1°. Examinador: Rodolfo Barros Chiaramonte

2°. Examinador: Paulo Augusto Nardi

Marília, 04 de dezembro de 2013.

DEDICATÓRIA

Aos meus pais, Cleudo e Elza, pelo sacrifício ilimitado em todos os sentidos, que mais do que me proporcionar uma boa infância, formaram os fundamentos do meu caráter e me apontaram o caminho a seguir. Obrigado por serem a minha referência de tantas maneiras e estarem sempre presentes na minha vida de uma forma indispensável.

A minha irmã Camila e família, que apesar de tantas provações esteve sempre disposta a me estender a mão e me oferecer ajuda, carinho, companhia. Que eu possa servir de exemplo para Lívia e Mariana (sobrinhas), para que elas possam seguir um caminho de luta e trabalho para conquistas de seus sonhos.

Aos meus familiares, que me apoiaram de todas as formas possíveis, incentivando, aconselhando em toda minha vida.

Aos amigos de perto e de longe, pelo amor e preocupação demonstrados através de ligações, visitas e e-mails. Obrigado, vocês que aliviaram minhas horas difíceis, me alimentando de certezas, força e alegria.

Muito obrigado, nunca será suficiente para demonstrar a grandeza do que recebi de vocês.

AGRADECIMENTOS

Ao Profº. Dr. Fábio Dacêncio Pereira, orientador, professor, amigo, pelo desprendimento ao escolher me dar apoio, muito obrigado pela dedicação e ajuda por esses anos de trabalho.

Agradeço ao Centro Universitário Eurípides de Marília – UNIVEM e ao *Computing and Information Systems Research Lab.* – COMPSI pelo incentivo, apoio e infraestrutura para a graduação e o desenvolvimento e conclusão deste projeto. Um agradecimento especial aos professores do COMPSI pela disponibilidade, esforço e dedicação para com os alunos, em especial a minha pessoa.

Agradeço ao Laboratório de Sistemas Integráveis Tecnológico – São Paulo/SP (LSI-TEC) e Profº Dr. Adilson Eduardo Guelfi pela oportunidade de estágio e o aprendizado no desenvolvimento do Assinador Digital ICP-Brasil e aprendizado "impar" em Assinatura Digital. Agradecimentos a toda equipe envolvida no desenvolvimento do projeto: Rodolfo Barros Chiaramonte, Éttore Leandro Tognoli e Cleverson Abreu Teotonio.

Agradecimentos a Boa Vista Serviços, administradora do SCPC, pelo estágio atual, pela oportunidade de aplicar conhecimentos adquiridos nestes anos de estudo e a oportunidade de aprendizado e crescimento na área da computação.

Sumário

Lista de Figuras

Lista de Siglas

ABRID - Associação Brasileira das Empresas de Tecnologia em Identificação Digital

AC - Autoridade Certificadora

AC-Raiz - Autoridade Certificadora Raiz

ACT - Autoridade de Carimbo de Tempo

AD-RA - Assinatura Digital com Referência para Arquivamento

AD-RB - Assinatura Digital com Referência Básica

AD-RC - Assinatura Digital com Referências Completas

AD-RT - Assinatura Digital com Referência de Tempo

AD-RV - Assinatura Digital com Referência para Validação

API - Application Programming Interface

AR - Autoridade de Registro

CAdES - Advanced Eletronic Signatures

CEF - Caixa Econômica Federal

CMS - Cryptographic Message Syntax

CNPJ - Cadastro Nacional da Pessoa Jurídica

COMPSI - Laboratório de Pesquisa em Computação e Sistemas de Informação – Marília/SP

CPF - Cadastro de Pessoa Física

CRL - Certificate Revocation List

ETSI - European Telecommunications Standards Institute

HTML - HyperText Markup Language

HTTP - Hypertext Transfer Protocol

ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira

ICP-Gov - Infraestrutura de Chaves Públicas do Poder Executivo Federal

IETF - Internet Engineering Task Force

IP - Internet Protocol

ITI - Instituto Nacional de Tecnologia da Informação

JNLP - Java Network Launching Protocol

JRE - Java Runtime Environment

LCR - Lista de Certificados Revogados

LSI-TEC - Laboratório de Sistemas Integráveis Tecnológico – São Paulo/SP

OCSP - Online Certificate Status Protocol

OSI - Open Systems Interconnection

QR-code - Quick Response

REST - Representational State Transfer

RFC - Request for Comments

RIA – Rich Internet Application

RIC - Registro de Identidade Civil

SDK - Software Development Kit

STF - Supremo Tribunal Federal

TCP - Transmission Control Protocol

UNCITRAL - United Nations Commission on International Trade Law

URI - Uniform Resource Identifier

URL – Uniform Resource Locator

XAdES - Advanced Eletronic Signatures

XML - Extensible Markup Language

XML-Dsig - Extensible Markup Language Digital Signature

WWW - World-Wide We

Resumo

Com o crescente avanço tecnológico e a necessidade de uso de tecnologias sustentáveis, vem sendo difundido e facilitado à substituição de documentos em papel pelos documentos eletrônicos. Para isso é necessário garantir a segurança da tramitação de informações contidas no documento eletrônico, tal segurança é obtida através da assinatura digital, tornando o documento seguro, íntegro e autêntico. Com a parceria do COMPSI e a LSI-TEC foi implementado um software completo para a assinatura digital no padrão ICP-Brasil desenvolvido em Java, onde se destaca a experiência no processo de desenvolvimento do assinador, verificador e ferramenta de carimbo de tempo. Propõe-se neste projeto a implementação de um *Web Service* para a assinatura digital.

Palavras Chave: ICP-Brasil; Assinatura Digital; Certificado Digital; Carimbo de Tempo; Serviço *Web*; JavaFX.

Abstract

The increasing technological advancement and the need for sustainable technologies spread and facilitate the replacement of paper documents for the electronic ones. For this purpose, it´s necessary to ensure the safe processing of the information contained in such documents. This security can be achieved through digital signature, which makes the document safe, integrate and authentic as well. With the partnership of COMPSI and LSI-TEC was implemented a complete software, developed in Java, for digital signature in the ICP-Brasil standard. It also highlights the experience in the development process of the signer, the verifier and the time stamp tool. This project proposes the implementation of a web service for the digital signature.

Keywords: ICP-Brasil; Digital Signature; Digital Certificate; Time Stamp; Web Service; JavaFX.

INTRODUÇÃO

Até os tempos atuais o homem registra por meio da escrita, mesmo que rudimentar, a autoria de uma obra ou propriedade por meio de uma assinatura. A palavra assinatura tem origem no latim “assignare” que significa afirmar, fazer verdadeiro o que está escrito antes. Com o uso e facilidades que o meio digital nos propicia, o avanço cada vez mais acentuado da tecnologia nos fornece um meio seguro e confiável de autenticação da informação, a assinatura digital.

Apesar da analogia com a assinatura manuscrita, a assinatura digital é elaborada e validada por sistemas computacionais, utilizando técnicas matemáticas e algoritmos criptográficos, e sua integração com outras soluções tecnológicas, como o certificado digital, permitiu não só a garantia de autenticidade, mas a integridade e o não-repúdio sobre um documento digital, fatores essenciais para que documentos eletrônicos sejam válidos na esfera jurídica, facilitando a economia de recursos tanto naturais quanto econômicos perante a sociedade.

Vários países se destacam por possuírem normas jurídicas a respeito da natureza e validade da certificação digital, aplicado principalmente no cenário que se encontra em constante evolução, o comercio eletrônico. O Brasil não ficou alheio ao desenvolvimento tecnológico referente à segurança da informação, tampouco aos seus avanços legislativos, e para garantir a autenticidade, a integridade e validade jurídica de documentos em forma eletrônica, cria-se um órgão governamental com o propósito de garantir a autenticidade e integridade de assinaturas digitais, a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), mediante a instituição da Medida Provisória 2.200-2, de agosto de 2001, incentivou a utilização da assinatura digital, ao dar presunção de veracidade aos documentos assinados sob a estrutura da ICP-Brasil, como visto nos seguintes trechos:

> *“Art. 1º Fica instituída a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.”*
> *(...).*
> *“Art. 10º Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.*
>
> > *§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do*

> *art. 131º da Lei nº 3.071, de 1 de janeiro de 1916 - Código Civil. (Medida Provisória 2.200-2, 2011).”*

Com a tendência de muitos serviços estarem migrando para o conceito de *Web Service*, devido ao ambiente *Web* ter se tornado o principal canal de comunicação e relacionamento de informações, surgiu a oportunidade de implementar o Assinador Digital ICP-Brasil como um serviço, desta maneira o usuário munido do seu certificado digital realiza uma requisição ao servidor e a *Application Programming Interface* (API) do Assinador Digital ICP-Brasil é carregado no *browser* do cliente, de modo que sua chave privada não trafegue na rede, para que o serviço seja consumido pelo cliente, onde é realizada a assinatura digital do documento.

Objetivos Gerais e Específicos

O presente trabalho de pesquisa tem como objetivo a implementação de um serviço disponibilizado na Internet para assinaturas de documentos digitais no modelo estabelecido pela ICP-Brasil, de modo a facilitar o acesso a tal tecnologia pela sociedade, provendo um grau satisfatório na segurança na assinatura de documentos digitais e validade no âmbito jurídico brasileiro.

Como objetivos específicos destacam-se:

- Estudo das tecnologias que envolvem o processo de assinatura digital;
- Estudo da regulamentação de assinatura digital de documentos eletrônicos proposta no âmbito da ICP-Brasil e válida no território brasileiro;
- Estudo dos conceitos de *Web Services*;
- Estudo da tecnologia JavaFX e suas características;
- Descrever o Assinador Digital ICP-Brasil, implementação de referência em Java, desenvolvido em parceria do LSI-TEC e o COMPSI; e
- Propor e desenvolver uma ferramenta que seja disponibilizada como um serviço via *Web*, seguindo as normas estabelecidas pela ICP-Brasil.

Metodologia

Primeiramente realizou-se estudos de trabalhos correlatos, o estudo da Medida Provisória nº. 2.200-2, de 24 de agosto de 2001 e seus conexos que regem o assunto.

Posteriormente o estudo mais aprofundado dos documentos emitidos pela ICP-Brasil sobre assinaturas digitais, certificados digitais e carimbo de tempo.

Para a concepção do projeto foi utilizada a *Integrated Development Environmen* (IDE) NetBeans 7.3.1 que consiste em uma IDE de código-fonte aberto e em uma plataforma de aplicativo, utilizada para construir qualquer tipo de aplicativo, incluindo melhorias continuas ao apoio para Groovy, PHP, C/C++ e JavaFX ([2]ORACLE, 2013).

A tecnologia JavaFX, desenvolvida pela Oracle baseada em Java, foi utilizada para o desenvolvimento do projeto, que atualmente se encontra na versão 2.2.21, escrita como uma API Java, o código em JavaFX pode referenciar APIs de qualquer biblioteca Java, permitindo a criação de aplicativos para *desktop*, *browser*, telefones celulares, entre outros, sendo totalmente integrados com *Java Runtime Environment* (JRE) ([1]ORACLE, 2013).

O JavaFX tem a capacidade de executar os aplicativos nela desenvolvidos dentro de um navegador *Web*. O aplicativo é executado dentro de uma máquina virtual Java, ou seja, é como implantar e iniciar o aplicativo em um navegador *Web*. Por este motivo tal tecnologia foi escolhida para o desenvolvimento do projeto, pois desta maneira é possível garantir a segurança da chave privada do assinante, de modo a assegurar que a chave privada não seja transmitida para o servidor.

Para a implementação do serviço de assinatura digital, além dos estudos realizados a respeito de conceitos e arquitetura *Web Service*, foi utilizado a API Assinador Digital ICP-Brasil desenvolvida em parceria da LSI-TEC e o COMPSI, que tem por finalidade auxiliar o desenvolvimento de aplicações para a assinatura de documentos eletrônicos e verificação de assinaturas digitais no âmbito da ICP-Brasil.

Organização do Trabalho

O primeiro capítulo apresenta a metodologia para geração da assinatura digital, bem como as tecnologias que apoiam a presunção de validade e segurança da assinatura gerada, como o certificado digital e carimbo de tempo.

O segundo capítulo apresenta uma breve introdução da história e cenário atual da assinatura digital no Brasil, referente sua validade no âmbito jurídico brasileiro. Apresenta a Infraestrutura da ICP-Brasil de modo ao entendimento de sua hierarquia e funções.

O terceiro capítulo apresenta o Assinador Digital ICP-Brasil, desenvolvido em parceria pelo LSI-TEC e o COMPSI, para o entendimento de seus módulos e os processos na geração da assinatura digital, seguindo as normas da ICP-Brasil.

O quarto capítulo aborda as tecnologias, conceitos e metodologia adotados para implementação do serviço de assinatura digital, bem como os testes realizados.

O quinto capítulo trata dos resultados obtidos da implementação e testes realizados, de modo a garantir os requisitos de segurança na geração de assinaturas digitais estabelecidos pela ICP-Brasil.

Por fim o ultimo capítulo apresenta as conclusões a respeito dos resultados obtidos, bem como as propostas de trabalhos futuros.

CAPÍTULO 1 - ASSINATURA DIGITAL

Diante do grande avanço tecnológico e mudança de hábito da sociedade deve-se tender à flexibilidade de conceitos antes consolidados. Um caso claro desta mudança é o conceito de documento tradicional, aposto em papel, que não mais se adequa a necessidade da sociedade, sendo evidentes suas limitações, em relação à agilidade de transmissão, conservação e segurança, sendo este o item que mais se discute. A assinatura digital surge com o propósito de garantir a segurança das informações contidas no documento eletrônico, sendo um método de autenticação digital tratada como análoga à assinatura física em papel, seu uso providência prova inegável de integridade e autenticidade do documento, para isso utilizam-se algumas técnicas de criptografia.

A privacidade é o ato de assegurar a não divulgação de informação entre duas partes a uma terceira parte externa as primeiras. Um dos princípios da criptografia é a integridade da informação; as ligações de comunicações eletrônicas estão sujeitas a erros e mesmo aos dados serem alterados. As técnicas criptográficas são usadas de modo a assegurar de que o conteúdo dos dados não mude quando forem transmitidos, do emissor para o receptor. Há duas técnicas criptográficas usadas para assegurar a privacidade da informação: a criptografia simétrica e a criptografia assimétrica:

- Criptografia Simétrica utiliza algoritmos criptográficos que fazem uso da mesma chave, tanto para cifrar quanto para decifrar a mensagem, neste tipo de algoritmo são usadas funções matemáticas bem complexas, com a finalidade de dificultar a recuperação da mensagem original por indivíduos não autorizados. O principal problema com a criptografia simétrica é o fato de que o emissor e o receptor devem possuir a mesma chave criptográfica, tendo que adotar métodos para transmissão e guarda de tal chave, conhecido com gerenciamento de chave.
- Criptografia Assimétrica utiliza um sistema criptográfico que utiliza um par de chaves matematicamente relacionadas, uma chave pública e outra privada, conhecida como criptografia de chave pública, o texto cifrado com a chave privada somente é decifrado com a chave pública, e vice-versa. A criptografia assimétrica surgiu para solucionar o problema com a segurança do compartilhamento da chave de criptografia.

  Uma categoria especifica de algoritmos que têm a função de tratar desse tipo de

serviço de segurança, são conhecidos como funções de *hash*. Uma função de *hash* utiliza dados binários, chamados de mensagem, e produz uma representação resumida, condensada, chamada de “resumo de mensagem”. Um *hash* é uma sequência de bits gerados por um algoritmo de *hash* que transforma a informação em uma cadeia de bits de mesmo tamanho, nesta operação não há volta, ou seja, não é possível obter a informação original a partir do *hash* gerado, esta sequência gerada tem a função de identificar uma informação de maneira única, onde qualquer alteração efetuada no arquivo, por mínimo que seja, altera o resultado do *hash*.

1.1. Assinatura Digital

Para obter a assinatura digital de um documento eletrônico são necessários dois tipos de processos criptográficos: o *hash* (resumo da mensagem) e a encriptação desse *hash*. Em um primeiro momento utilizando-se de algoritmos de criptografia (SHA-256, SHA-512, os mais comuns utilizados no momento) obtém-se o resumo da mensagem original, que nada mais é do que a transformação das informações de um documento em uma sequência de *bits* (ICP-Brasil, 2012).

Após a obtenção do *hash*, é feita a criptografia deste *hash* utilizando um modelo específico, a criptografia assimétrica (chave pública e chave privada), em que o autor da mensagem utiliza sua chave privada para criptografar o resumo da mensagem e armazenar o *hash* gerado junto à mensagem original, obtendo assim a assinatura digital. Para verificar a autenticidade e integridade do documento, o receptor gera um *hash* a partir da mensagem original, e decriptografa a assinatura digital utilizando a chave pública do autor. Assim, comparando-os, se os dois *hashes* forem idênticos o documento é válido e não foi modificado, caso contrário, alguma violação ocorreu na mensagem (ICP-Brasil, 2012). Na figura 1 encontra-se a esquematização das etapas da assinatura digital.

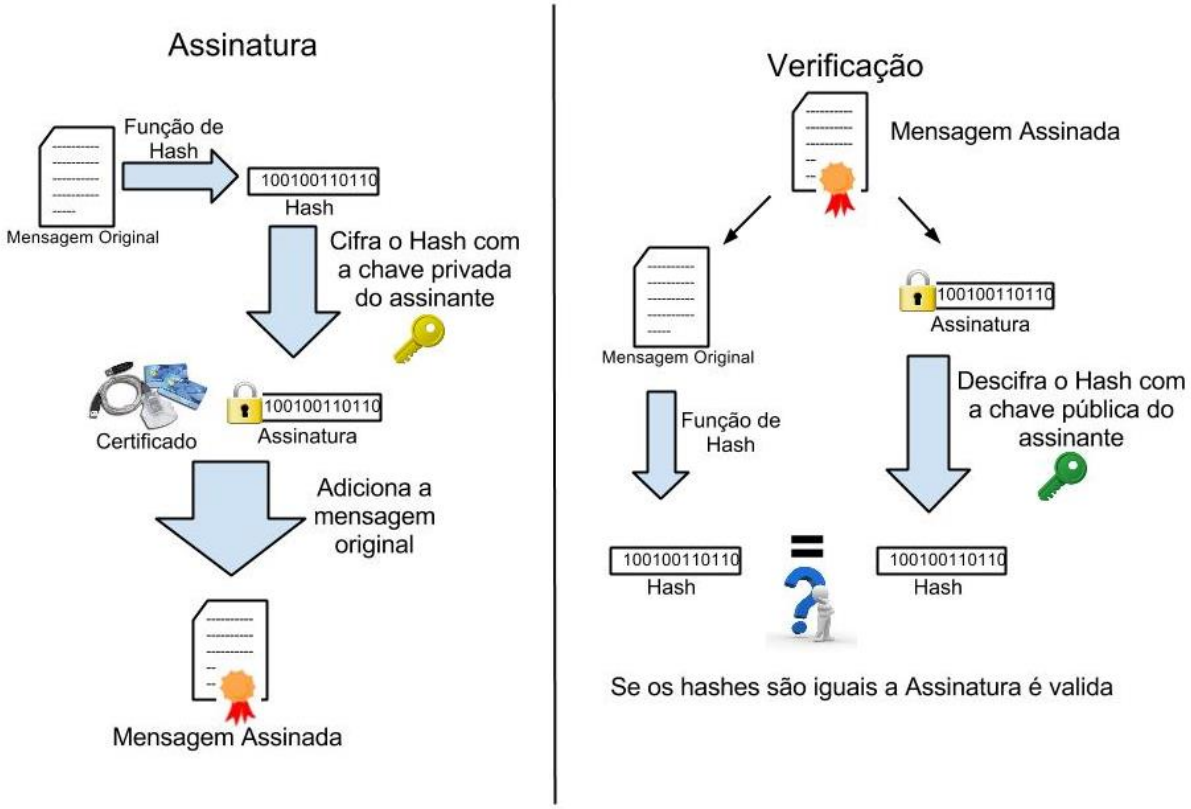

Figura 1. Esquematização das etapas de Geração e Validação da Assinatura Digital. (Própria).

A ICP-Brasil adotou um perfil definido em dois padrões internacionais para a geração da assinatura digital: *Cryptographic Message Syntax* (CMS) *Advanced Eletronic Signatures* (CAdES) e *Extensible Markup Language Digital Signature* (XML-DSig) *Advanced Eletronic Signatures* (XAdES), que contém um subconjunto dos atributos/propriedades incorporando as principais informações julgadas relevantes. De acordo com a documentação da ICP-Brasil a adoção deste padrão tem o objetivo de minimizar as diferenças entre implementações e maximizar a interoperabilidade (ICP-Brasil, 2012), atribuindo, deste modo, uma padronização das aplicações para geração e verificação das assinaturas digitais no contexto brasileiro.

A ICP-BRASIL criou seus formatos de assinaturas digitais com base nas padronizações *European Telecommunications Standards Institute* (ETSI), que fornece uma padronização de como se deve gerar e codificar uma assinatura digital, que se fundamenta nos padrões para *Internet* desenvolvidos pela *Internet Engineering Task Force* (IETF) conhecidos como *Request for Comments* (RFC). A figura 2 ilustra, de forma sucinta, a estrutura dos formatos de assinaturas ICP-Brasil: Assinatura Digital com Referência Básica (AD-RB); Assinatura Digital com Referência de Tempo (AD-RT); Assinatura Digital com Referência para Validação (AD-RV); Assinatura Digital com Referências Completas (AD-RC) e

Assinatura Digital com Referência para Arquivamento (AD-RA), sendo o formato mais completo de assinatura digital.

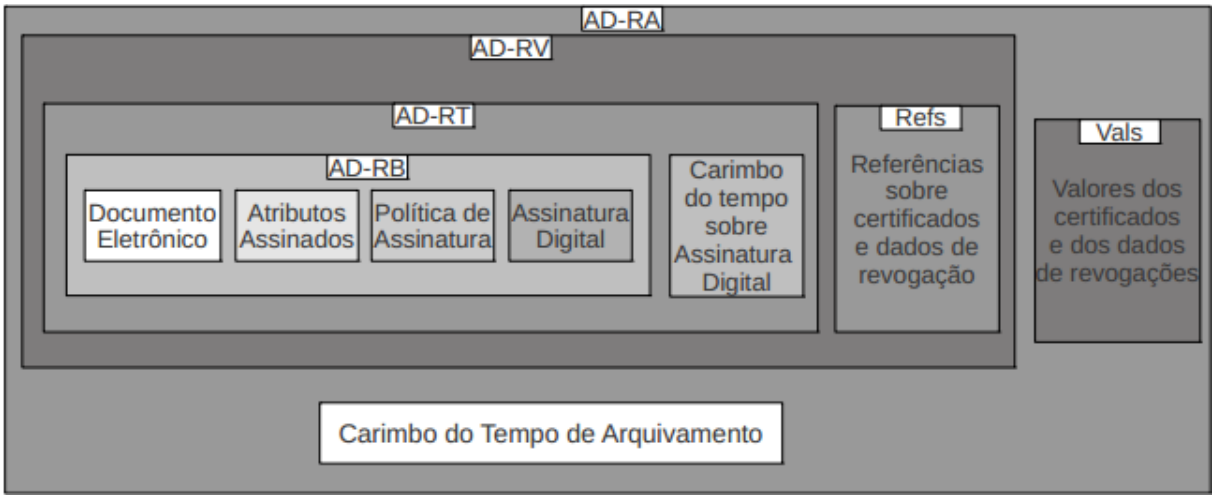

Figura 2. Estrutura dos Formatos de Assinaturas ICP-Brasil. (ICP-Brasil, 2012).

O processo de geração das assinaturas digitais na ICP-Brasil prevê quatro contextos distintos: a) assinaturas simples (quando uma única assinatura é gerada sobre o documento eletrônico); b) contra-assinaturas; c) co-assinaturas e; d) assinaturas em lote (quando uma assinatura é gerada sobre vários documentos ao mesmo tempo).

A geração de contra-assinaturas digitais ocorre quando uma ou mais assinaturas digitais são realizadas sobre uma sequência de *bytes*, que representa uma assinatura digital já existente, ou seja, a assinatura de uma assinatura digital.

A geração de co-assinaturas digitais ocorre quando duas ou mais assinaturas digitais são geradas de forma independente pelos signatários utilizando conteúdos digitais idênticos.

Cada co-assinatura ou contra-assinaturas geradas podem conter atributos próprios, assinados e não assinados. Este procedimento é realizado acrescentando informações do novo assinante à estrutura do arquivo digital. Trata-se de um processo aceitável e homologado, pois não compromete a segurança tanto do documento em si como de outras assinaturas digitais contidas no documento. No entanto, resguarda a Instrução Normativa do Instituto Nacional de Tecnologia da Informação (ITI) que contra-assinaturas não devem ser empregadas após a aposição de qualquer carimbo do tempo de arquivamento devido à interferência no processo de validação (Alves *et al*, 2013).

1.2. Carimbo de Tempo

Em algumas transações de documentos eletrônicos assinados digitalmente, torna-se necessária à inclusão de informações sobre a data/hora em que o processo foi realizado. Neste contexto surgiu a importância de agregar o fator tempo aos documentos eletrônicos assinados.

As referências temporais são pontos chave nas operações relacionadas à assinatura digital. Existem três referências temporais: a) aquelas relacionadas ao instante da assinatura; b) aquelas relacionadas ao intervalo de validade do certificado digital e; c) aquelas relacionadas ao intervalo de validade de uso do certificado digital.

Para tanto, alguns intervalos de tempo devem ser respeitados para o processo de validação da assinatura digital: a) o instante da realização do processo de assinatura digital necessita estar no período válido do certificado digital; b) a assinatura digital deverá ser realizada antes de uma possível data de revogação do certificado digital e; c) o instante de início de validação do certificado necessita ser menor do que o instante do término da validação do certificado (Alves *et al*, 2013), como ilustrado na figura 3.

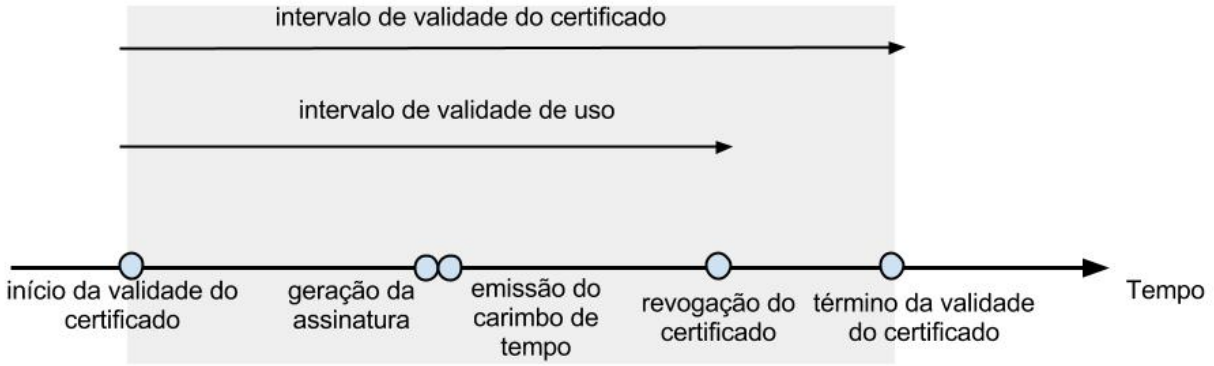

Figura 3. Referências temporais dos processos de assinaturas. (Adaptado ICP-Brasil, 2009).

Algumas referências temporais devem ser emitidas por fontes seguras como: a) início e término da validade do certificado digital (Autoridades Certificadoras); b) instante de revogação do certificado digital do signatário (Autoridades Certificadoras) e; c) instante de emissão do carimbo de tempo (Autoridades Certificadoras de Tempo).

Garantindo as fontes seguras de tempo citadas anteriormente, o instante da formalização da assinatura pode ser gerado por uma fonte não confiável como, por exemplo, a data/horário do microcomputador onde foi gerada a assinatura do documento eletrônico.

Diante deste contexto surgiu o conceito de carimbo de tempo, que é a forma segura e confiável de agregar e registrar a data e hora em transações de documentos eletrônicos, em especial os assinados digitalmente, obtendo prova que tal documento assinado existia na data incluída no carimbo de tempo.

1.3. Certificado Digital

Pode-se observar que um dos pontos críticos da assinatura digital é a garantia de que tal assinatura pertence realmente à pessoa que a utiliza, ou seja, que a chave pública e privada pertence realmente ao emissor da mensagem assinada. Diante deste panorama, necessita-se de uma terceira parte confiável, que garanta tais informações, o certificado digital surge com esse propósito.

O certificado digital, além de personificar um indivíduo ou entidade na rede mundial de computadores, garante, por força da legislação atual (Medida Provisória, 2001) validade jurídica aos atos praticados com seu uso. A certificação digital permite que transações feitas de forma virtual sejam realizadas, ou seja, sem a presença física do interessado, mas que garante a identificação clara da pessoa que a está realizando. Os certificados digitais podem ser destinados para assinaturas, cujo objetivo é confirmar a identidade em uma operação eletrônica, ou assinaturas e sigilo em diferentes níveis, que delimitam a segurança atribuída ao certificado digital e servem para cifrar documentos, base de dados e outras informações eletrônicas (Freitas e Loebens, 2004).

Na prática, o certificado digital equivale a uma carteira de identidade virtual, ao permitir a identificação de uma pessoa no meio digital/eletrônico, conferindo assim validade legal ao documento e identificação inequívoca. O certificado digital é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas pelo ICP-Brasil e auditada pelo ITI, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas (ITI, 2013). A figura 4 mostra a interface do certificado digital no sistema operacional *Windows*.

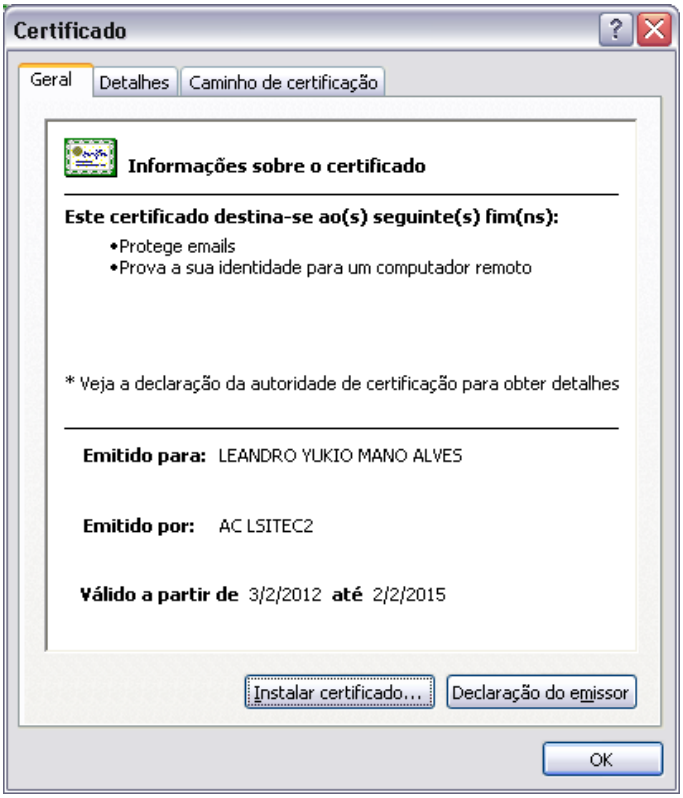

Figura 4. Certificado Digital. (Própria).

Quanto aos certificados digitais, de acordo com a Resolução nº. 41, de 18 de abril de 2006 do Comitê Gestor da ICP-Brasil, o qual aprovou requisitos mínimos para as políticas de certificados ICP-Brasil, são oito os tipos de certificados de usuários finais, sendo A1, A2, A3 e A4 utilizados para assinatura digital e S1, S2, S3 e S4 utilizados para sigilo de informações, onde as escalas de 1 a 4 definem o nível de segurança, onde os tipos A1 e S1 são níveis menos rigorosos que os A4 e S4, vale ressaltar que os certificados do tipo A3, as chaves criptográficas são geradas e armazenadas em um *token*, como por exemplo, um *smart card* (cartão inteligente), tornando possível o transporte do certificado e assinatura de documentos onde desejar, garantindo maior segurança, pois seus dados permanecem invioláveis e únicos, não permitindo exportação ou qualquer tipo de reprodução de informações (Resolução nº 41, 2006).

O Certificado de Atributo é a mais recente tecnologia padronizada pela ICP-Brasil para agregar mais valor às aplicações eletrônicas que se utilizam da certificação digital, sendo um documento eletrônico assinado, garante todas as prerrogativas legais e técnicas, ou seja, integridade, autenticidade, não-repúdio e valor legal. Segundo Ramos o Certificado de Atributo permite de fato quem tem a prerrogativa legal de dar ou atribuir alguma qualificação

para alguém ou alguma coisa, possa assim fazê-lo (Ramos, 2013). Assim as entidades responsáveis legalmente por emitir/atribuir atributos necessita apenas de um certificado digital.

Um caso de sucesso na aplicação do Certificado de Atributo é a emissão do documento aos estudantes, por meio de um acordo entre as entidades que representam os estudantes e a Associação Brasileira das Empresas de Tecnologia em Identificação Digital (ABRID), com a anuência do ITI. Desta maneira atribui mais segurança e confiabilidade ao novo cartão de identificação do estudante, sendo que ele vem com *Quick Response* (QR *code*) e certificado digital de atributo no padrão ICP-Brasil.

1.4. Considerações Finais do Capítulo

A assinatura digital surge como uma forma de transmitir segurança a um documento eletrônico, de modo a garantir sua integridade, autenticidade e não-repúdio.

O Brasil, por intermédio da ICP-Brasil, criou os formatos de assinaturas digitais, com base em padrões internacionais, de modo a minimizar diferenças entre implementações e maximizar a interoperabilidade, estabelecendo um padrão para a geração e verificação das assinaturas digitais. Pode-se notar que alguns formatos estabelecidos pela ICP-Brasil exigem um carimbo de tempo, incluindo a data e hora na assinatura digital do documento eletrônico, agregando mais valor e confiabilidade ao mesmo. Por fim a necessidade da utilização do certificado digital, emitido pela ICP-Brasil, permitindo a identificação de uma pessoa no meio eletrônico, que tem o propósito de garantir que tal assinatura digital pertence à pessoa que a utiliza.

Desta maneira, o uso da assinatura digital, carimbo de tempo e certificado digital transmitem a segurança necessária para o processo de assinatura digital de documento eletrônico.

CAPÍTULO 2 - ASPECTOS JURÍDICOS DA ASSINATURA DIGITAL NO BRASIL

Diante da realidade da tecnologia da informação, fornecer suporte para que os atos realizados no meio tradicional possam, também, ser realizados no meio ambiente eletrônico, tem-se por objetivo enfrentar a questão de como os tribunais superiores vêm se posicionando diante da hipótese de assinatura digital divergente daquele que efetivamente assinou o documento digitalizado, sobretudo em face dos critérios da garantia de confiabilidade, identificação, integridade e o não-repúdio (Devegili, 2001). Assim como apontar eventual falha dos sistemas por conta da não adoção de uma autoridade certificadora de tempo, indispensável para verificar, em tempo real, a validade do certificado digital.

Assim, por meio de uma revisão bibliográfica, legislativa e jurisprudencial, buscar-se-á analisar o sistema da ICP-Brasil, como alicerce para discutir criticamente os julgados dos tribunais superiores, e verificar se, efetivamente, a tecnologia da informação é capaz de resolver a questão da assinatura digital eletrônica e a validade do certificado digital em tempo real.

2.1. Critérios de Validade Jurídica do Documento Eletrônico

Preocupada com a questão da autenticidade e veracidade do documento eletrônico, a *United Nations Commission on International Trade Law* (UNCITRAL) sedimentou, no ano de 2001, o *Model Law on Eletronic Signatures* enquanto uma diretriz a ser seguida para a regulamentação de atos jurídicos, nomeadamente àqueles voltados às transações comerciais *online*. Adotou o critério da neutralidade quanto às regras técnicas para estabelecer firmas eletrônicas, aprovando qualquer método ou técnica comprovadamente eficaz e segura (Guimarães *et al*, 2005).

Nesta época, vigorava no Brasil o Decreto nº 3.587, de 5 de setembro de 2000 (Decreto nº 3.587, 2000), que instituiu normas para a Infraestrutura de Chaves Públicas do Poder Executivo Federal (ICP-Gov) e estipulou a necessidade de uso da criptografia assimétrica para relacionar um certificado digital a um indivíduo ou a uma entidade enquanto ferramenta para garantir segurança na tramitação de documentos entre os órgãos do governo. O objetivo era viabilizar a oferta de serviços de sigilo, validade, autenticidade e integridade de dados, irrevogabilidade e irretratabilidade das transações eletrônicas e das aplicações de

suporte que utilizam certificados digitais.

O referido decreto serviu de alicerce para instituição da Medida Provisória nº 2.200-2, de 24 de agosto de 2001 (Medida Provisória, 2001), que estabeleceu o sistema de ICP-Brasil, com o objetivo de garantir autenticidade, integridade e validade jurídica de documentos eletrônicos. Ampliou-se, assim, o alcance e aplicação da certificação digital, agora não mais restrita ao âmbito da Administração Pública Federal. De acordo com Custódio, a ICP-Brasil compreende um conjunto de técnicas, práticas e procedimentos com o objetivo de fornecer suporte à implementação e à operação de um sistema de certificação (Custódio, 2001).

O Decreto nº 3.996, de 31 de outubro de 2001 (Decreto nº 3.996, 2001), revogou expressamente o Decreto nº 3.587, de 5 de setembro de 2000 (Decreto nº 3.587, 2000), e passou a estipular que os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da ICP-Brasil. Modificado pelo Decreto nº 4.414, de 7 de outubro de 2002 (Decreto nº 4.414, 2002), estabeleceu que as aplicações e demais programas utilizados no âmbito da Administração Pública Federal, direta e indireta, que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitido por qualquer AC integrante da ICP-Brasil.

Para o documento servir como prova, há necessidade de que o pensamento humano esteja materializado em um suporte, em cujo contexto se insere o eletrônico, e que a manifestação do pensamento humano sirva para comprovar algo. Dentro deste contexto, a identificação da autoria do documento é um dos requisitos para conferir força probante ao documento. No âmbito eletrônico, Volpi (Volpi, 2001) salienta que:

> *Para a prevenção deste tipo de situação, surgiu a certificação digital. Seu funcionamento pode ser comparado a de um serviço notarial efetuado pelo tabelião. Fundamenta-se na existência de uma autoridade certificadora, responsável pela emissão do certificado digital, que possui registrado, em sua base de informações, a chave pública usada para decifrar a mensagem - criptoanálise do emissor do documento. Por meio de mecanismos próprios, a autoridade certificadora pode identificar como original o documento do emissor e, a partir desta comprovação, certificar, com uma assinatura digital própria, a autenticidade do documento eletrônico.*
>
> O documento eletrônico, com sua assinatura digital e seu respectivo certificado digital,

é empregado por apresentar segurança ao poder judiciário, devido ao seu alto grau de complexidade, nomeadamente em relação à criptografia assimétrica, garantindo assim a autoria e integridade do documento. A assinatura digital é o mecanismo de autenticação que permite ao criador de uma mensagem anexar um código que atue como uma assinatura (Stallings, 2008). Esse tipo de assinatura possui o mesmo valor de uma assinatura manuscrita, portanto somente as assinaturas digitais realizadas com certificados emitidos por autoridades credenciadas na ICP-Brasil tem validade jurídica reconhecida.

Apesar do tratamento análogo com a assinatura manuscrita, a assinatura digital é elaborada e validada por sistemas computacionais em que se utilizam técnicas matemáticas e algoritmos criptográficos, e sua integração com outras soluções tecnológicas, como o certificado digital, permite não só a garantia de autenticidade, mas a integridade e o não-repúdio sobre um documento digital.

Para a garantia da eficácia da assinatura digital e de sua certificação, dois aspectos merecem ser observados: a segurança das informações que individualizam cada indivíduo e a segurança da chave privada de cada certificado. Embora ambos os elementos sejam essenciais para a segurança da assinatura digital, o sujeito passivo se distingue da obrigação da segurança das informações.

Quanto à segurança das informações individuais, a responsabilidade compete ao Poder Público, através da ICP-Brasil, mas a segurança da guarda da chave privada compete exclusivamente ao proprietário do certificado digital. Essa distinção é importante, pois aponta o possível responsável pela reparação de danos causados a outrem provenientes de fraudes na utilização do certificado digital emitido pela ICP-Brasil. Ressalta-se que o documento eletrônico é passível de fraude assim como o documento tradicional. No entanto, o que se pretende com a assinatura digital é minimizar a possibilidade de fraude e identificá-la quando ocorrer, o que se traduz em maior segurança jurídica.

2.2. Infraestrutura da ICP-Brasil

A Medida Provisória nº 2.200-2/2001 (Medida Provisória, 2001) transformou o ITI em autarquia federal e o vinculou ao Ministério da Ciência e Tecnologia, com a função de Autoridade Certificadora Raiz (AC-Raiz). O ITI passou a ser a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais

aprovadas pelo Comitê Gestor da ICP-Brasil, tendo como função credenciar e fiscalizar as entidades integrantes da ICP-Brasil.

Diferentemente do sistema americano, pontuado pela autonomia das autoridades certificadoras, a ICP-Brasil possui uma estrutura hierárquica. Afora a AC-Raiz, a estrutura é composta pelas ACs, entidades credenciadas a emitir certificados digitais vinculando pares criptográficos ao respectivo titular, com a incumbência de emitir, expedir, distribuir, revogar e gerenciar certificados, publicar listas de certificados revogados e outras informações pertinentes, além de manter registro de suas operações, bem como a Autoridades de Registro (AR), operacionalmente vinculadas a uma AC, com competência para identificar e cadastrar usuários presenciais, encaminhar solicitações de certificados às ACs e manter registros das operações eletrônicas (Medida Provisória, 2001).

Quaisquer entidades públicas e as pessoas jurídicas de direito privado poderão ser credenciadas como AC e AR. Proíbe-se, no entanto, a AC certificar nível diverso do imediatamente subsequente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, aprovados pelo Comitê Gestor da ICP-Brasil. A figura 5 ilustra a estrutura resumida da ICP-Brasil, apenas com as ACs de 1º nível e de 2º nível, atualizada 31/10/2013.

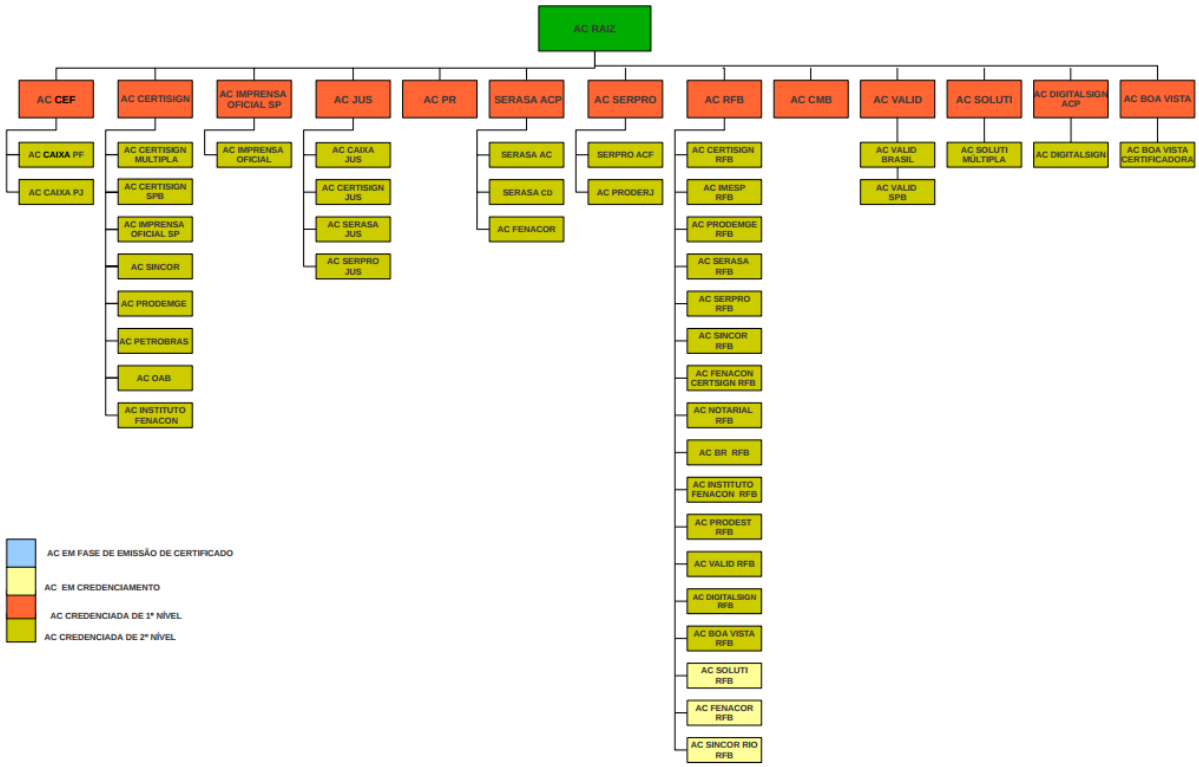

Figura 5. Estrutura Resumida da ICP-Brasil. (ITI, 2013).

2.3. Autoridade de Carimbo de Tempo

Em 19 de novembro de 2008, a ICP-Brasil aprovou as normas para implementação de Autoridade de Carimbo de Tempo (ACT), que permite determinar data/hora da assinatura digital. O Carimbo de Tempo é uma assinatura digital de um terceiro confiável que garante que um documento existia em determinada data, desta forma é possível assinar documentos digitalmente anexando data e hora específica, garantida pelo Observatório Nacional, que é responsável pelo fornecimento da hora legal no Brasil, que possui infraestrutura de segurança obedecendo aos mais altos padrões mundiais (ICP-Brasil, 2009). O modelo geral de funcionamento da ACT está representado na figura 6.

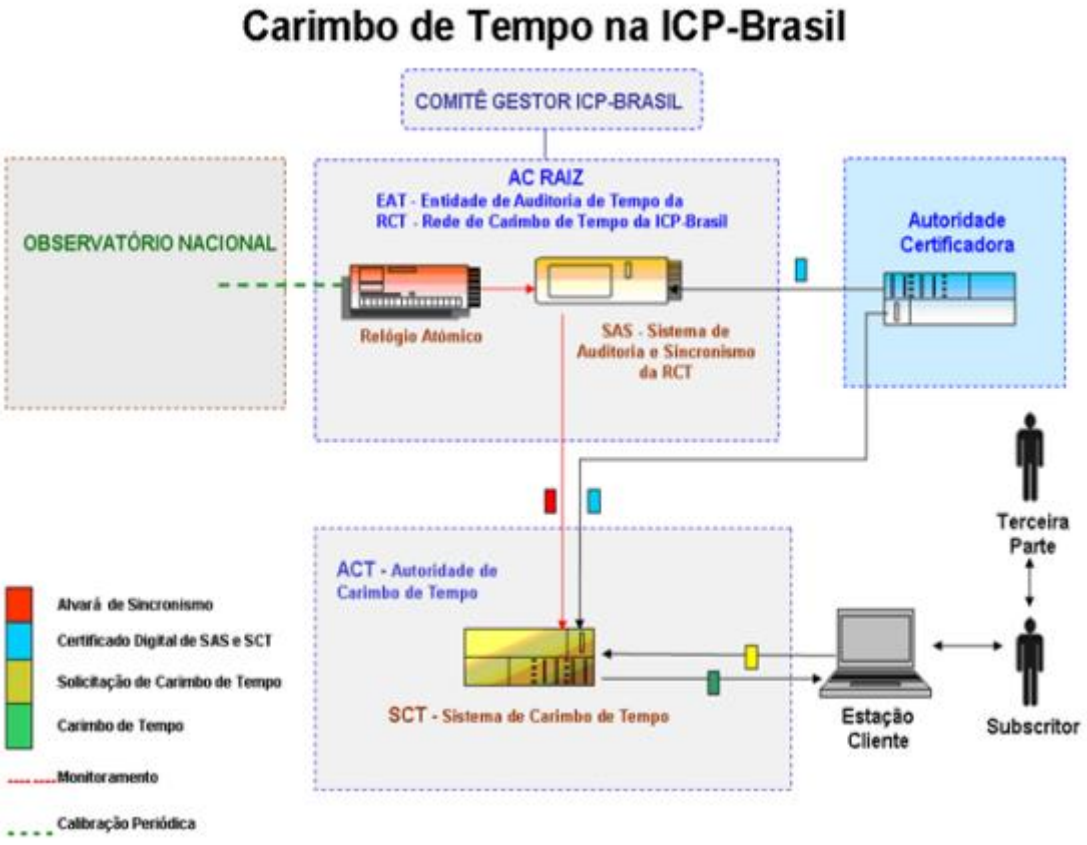

Figura 6. Modelo de Funcionamento do Carimbo de Tempo da ICP-Brasil. (ICP-Brasil, 2010).

Apesar da utilização de carimbos de tempo ser facultativa no âmbito da ICP-Brasil, as referências temporais são elementos obrigatórios na geração de alguns formatos de assinaturas digitais, somente a política de assinatura básica não faz uso de carimbos de tempo.

No dia 28 de janeiro de 2013 foi publicado no Diário Oficial da União o

credenciamento da Caixa Econômica Federal (CEF) como a primeira Autoridade de Carimbo de Tempo da ICP-Brasil. Segundo Renato Martini, diretor-presidente do ITI, com o credenciamento da ACT CAIXA, a AC-Raiz passa a operar suas instalações enquanto raiz do tempo da ICP-Brasil, tratando de mais um atributo de confiança em prol a adoção de documentos e processos eletrônicos. Inicialmente a ACT CAIXA somente emitiram carimbos de tempo aos processos de assinaturas digitais referentes às áreas internas da CEF que necessitam da comprovação temporal (CAIXA, 2013).

O uso de carimbo de tempo é uma realidade desde maio de 2007 no judiciário. O Supremo Tribunal Federal (STF) recebe e tramita processos de forma totalmente eletrônica. Para atestar a data e o horário em que os processos chegam ao sistema, o Tribunal utiliza uma solução de carimbo do tempo. O sistema de petição eletrônica, com certificação digital ICP-Brasil do STF, é utilizado inclusive para as petições iniciais (as que darão início a uma ação judicial) e para todos os tipos de classes processuais e, também, aos processos de suporte ainda em papel. Nessas petições é utilizado o carimbo de tempo para aferir com exatidão o horário desta transação eletrônica (Alves *et al*, 2013).

2.4. Considerações Finais do Capítulo

A instituição da Medida Provisória 2.200-2 estabelece toda a infraestrutura da ICP-Brasil, de modo a normatizar e padronizar as competências das entidades que compõem a ICP-Brasil.

Desta maneira os documentos eletrônicos que possuem assinaturas digitais geradas com certificados digitais emitidos pela ICP-Brasil e de acordo com as normas estabelecidas pela mesma, possuem o mesmo valor jurídico de documentos em papel, garantida por lei vigente, de modo que possam substituir os documentos em papel pelos documentos eletrônicos.

CAPÍTULO 3 - ASSINADOR DIGITAL ICP-BRASIL

Desenvolvido em parceria pelo Laboratório de Sistemas Integráveis Tecnológico – São Paulo/SP (LSI-TEC) e pelo Laboratório de Pesquisa em Computação e Sistemas de Informação (COMPSI), o Assinador Digital ICP-Brasil (Alves *et al*, 2012) permite a realização de assinaturas digitais de documentos eletrônicos e a verificação das assinaturas e respectivos certificados presentes em um documento assinado digitalmente. Para isso, esse *software* foi dividido em quatro módulos, que juntos compõem os serviços de assinatura que atendem os requisitos da ICP-Brasil.

3.1. Módulos de Verificação e Validação

Os módulos de verificação e validação são responsáveis por analisar os certificados digitais no processo de assinatura e a validação de documentos já assinados, respectivamente. Em um certificado digital deve-se verificar sua assinatura, validade, revogação e sua cadeia de certificados. São inúmeros os requisitos de verificação exigidos pela ICP-Brasil, sendo que alguns deles são discriminados sucintamente a seguir:

- Assinatura: a partir das informações contidas no próprio certificado, deve ser obtido o certificado de sua AC. Os campos que auxiliam na obtenção dos certificados são: o *"Issuer"* e o *"Authority Information Access"*; que são respectivamente o nome da AC e *Uniform Resource Locato*r (URL) para realizar o *download* do certificado ou realizar uma verificação via *Online Certificate Status Protocol* (OCSP). Após a obtenção do certificado de sua AC, deve ser feito a verificação criptográfica do certificado, que consiste em aplicar a função de *hash* definida, nos campos assinados do certificado, decifrar a assinatura com chave pública da AC e comparar os resultados obtidos.

- Validade: o certificado possui duas datas que definem um período de validade, estas datas devem ser validas, e o período determinado deve estar contido no período de validade de sua AC.

- Lista de Certificados Revogados (LCR): deve-se possuir a LCR mais recente do certificado, para saber se este foi revogado e quando, o certificado possui um campo que auxilia a localização de tal lista, o *Certificate Revocation List* (CRL) *Distribution Points*, que contem URL's para realizar o *download* da versão da lista atualizada.

- Cadeia: todos os processos descritos anteriormente devem ser realizados para as ACs de forma recursiva, até a AC-Raiz.

Um certificado ICP-Brasil possui algumas validações específicas para representar uma pessoa jurídica ou uma pessoa física. Sendo assim um certificado para pessoa jurídica precisa ter os seguintes campos: nome, número do Cadastro de Pessoa Física (CPF), data de nascimento do responsável pelo certificado e o número do Cadastro Nacional da Pessoa Jurídica (CNPJ) da empresa, e para uma pessoa física, seu nome e número do CPF, sendo opcionais alguns outros dados, como título de eleitor, zona eleitoral, *e-mail* e Registro de Identidade Civil (RIC).

O *software* desenvolvido se propõe a analisar certificados digitas, fazendo as validações básicas e as verificações mais restritas propostas pela ICP-Brasil, gerando uma lista das possíveis anomalias do certificado, auxiliando na normalização das emissões e uso dos certificados regulamentados pela ICP-Brasil (Alves *et al*, 2012).

3.2. Módulo Assinador

Os cinco formatos de assinatura digital regulamentada pela ICP-Brasil possuem um processo de geração cumulativa, ou seja, para se gerar um AD-RT é preciso partir de um AD-RB, e assim sucessivamente, porém novos atributos são incorporados, como é o caso do Carimbo de Tempo das Referências, que é obrigatório no AD-RC e optativo no AD-RA. Importante ressaltar que foi adotado para o desenvolvimento do software o formato CAdES, e sua codificação pode ser binária: BER/DER; ou texto: Base64. Todos os processos pertinentes à geração, anexação e codificação da assinatura digital são definidos pela ICP-Brasil, a figura 7 ilustra o fluxo básico da geração de um arquivo assinado.

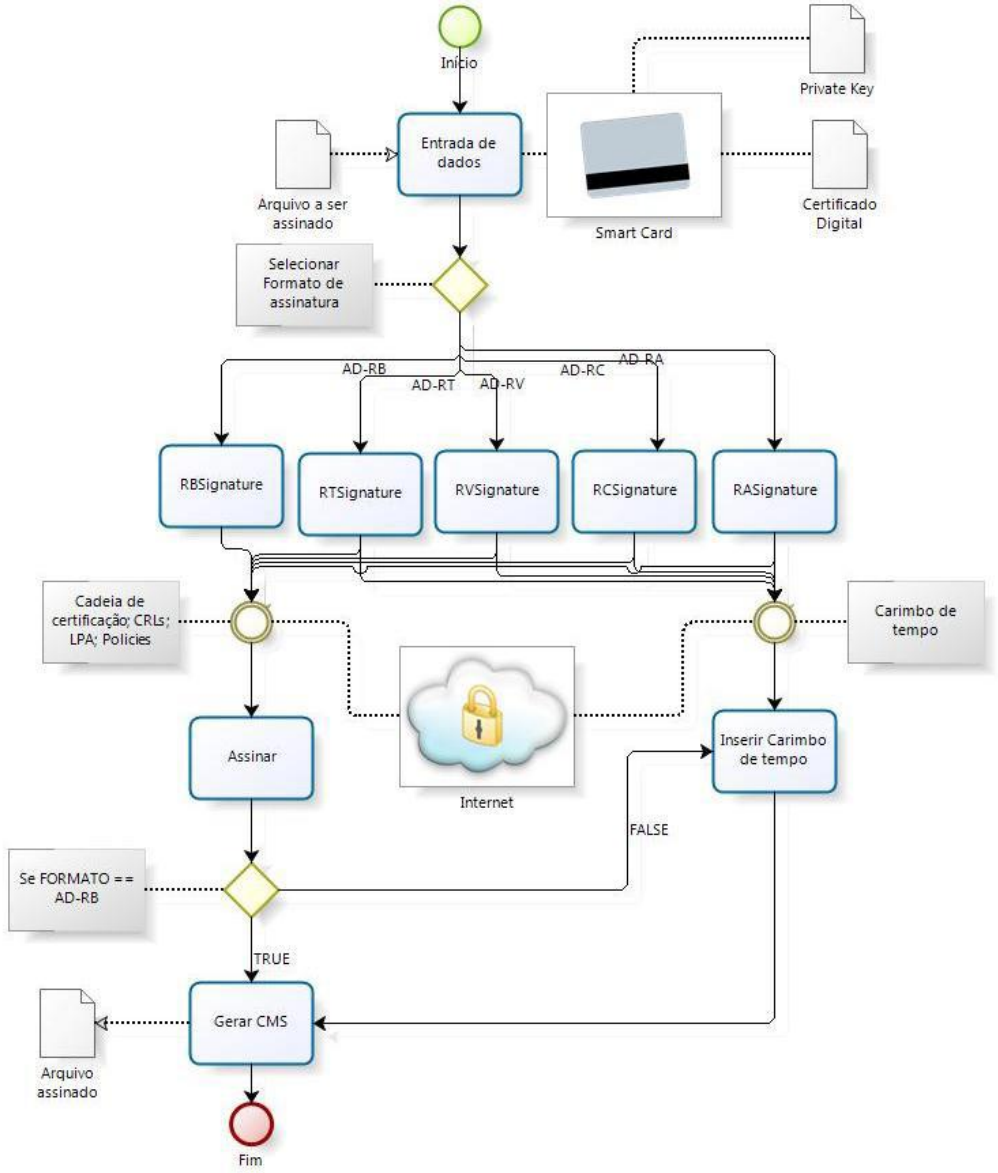

Figura 7. Fluxo Básico da Geração de um Arquivo Assinado. (Alves *et al*, 2012).

O CMS é a estrutura básica de um documento eletrônico assinado, é construído a partir de dados de entrada, como certificado digital e um arquivo eletrônico a ser assinado. O *software* assinador digital desenvolvido gera o documento eletrônico assinado a partir do certificado digital e da chave privada, ambos contidos no *smart card*, e constrói um CMS de acordo com o formato de assinatura selecionado, são consultados em repositórios *online* informações como cadeia de certificação, LCRs e *policies*, gerando ao seu final o documento assinado (Alves *et al*, 2012).

3.3. Módulo Carimbador

Para amenizar os custos de projeto e aprendizado sobre o assunto foi usado o *SignServer* (SignServer, 2012), que é uma ferramenta utilizada para executar operações criptográficas, onde o gerenciamento de chaves criptográficas é desejado. O *SignServer* vem com um *plugin* para um servidor de carimbo de tempo, compatível com *Request for Comments* (RFC) 3161 e é usado para gerar carimbos de tempo assinados digitalmente. Algumas modificações foram realizadas para o carimbador de tempo pudesse estar em acordo com o documento emitido pela ICP-Brasil, REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL DOC-ICP-12 - versão 1.1 13 de outubro de 2009, onde prevê requisitos para que os carimbos de tempo emitidos pelas ACTs estejam nas normas aceitas pela ICP-Brasil (ICP-Brasil, 2009). Desta maneira foi criada uma ACT *fake* para emissão dos carimbos de tempo, disponibilizada para interessados e testes referentes ao assunto no endereço eletrônico
http://act.compsi.univem.edu.br/signserver/process?workerName=TimeStampSigner.

Em um primeiro instante foi criada uma ferramenta em Java que realiza a requisição de carimbo de tempo a ACT e inclui o *TimeStampToken*, atributos assinados e atributos não-assinados no CMS. Depois de analisar a estrutura e padrões do carimbo de tempo emitido, este foi adicionado no projeto principal, que visa assinar documentos nos formatos definidos pela ICP-Brasil que necessitam do carimbo de tempo para serem validados (AD-RT, AD-RV, AD-RC e AD-RA).

3.4. Considerações Finais do Capítulo

Com o auxílio da API Assinador Digital ICP-Brasil, desenvolvida pelo LSI-TEC e o COMPSI, é possível a implementação de um serviço para disponibilizar o processo de assinatura digital de documentos eletrônicos válidos no âmbito jurídico brasileiro, pois seguem as normas estabelecidas pela ICP-Brasil. O próximo capítulo apresenta as tecnologias e arquitetura para o desenvolvimento do serviço de assinatura digital ICP-Brasil.

CAPÍTULO 4 – CONCEITOS E ARQUITETURA DO SERVIÇO DE ASSINATURA DIGITAL ICP-BRASIL

A *World-Wide Web* (WWW), ou simplesmente *Web* é um espaço de informação onde os recursos, são identificados por chaves globais chamadas de *Uniform Resource Identifier* (URI) ([1]W3C, 2004). A iniciativa que tornou possível a *Web* ser o que é hoje foi tomada por Tim Berners-Lee em 1980 na Suíça. Sua intenção original era tornar mais fácil o compartilhamento de documentos de pesquisas entre seus colegas. Ainda que diferente do modelo de *Web* atual, o projeto inicial continha algumas das mesmas ideias adotadas atualmente, utilizando como base os padrões URI, *HyperText Markup Language* (HTML) e *Hypertext Transfer Protocol* (HTTP). Segundo Berners-Lee, o sistema de identificação URI disponibiliza uma forma simples e extensível de identificar recursos; como páginas *Web*, imagens, vídeos e serviços (Berners-Lee *et al*, 2005).

A maioria dos protocolos de recuperação e envio de representações faz uso de uma sequência de uma ou mais mensagens, que juntas contêm os dados e metadados de uma representação a ser transferida entre agentes (navegador/servidor). Atualmente, o protocolo de comunicação *Transmission Control Protocol* (TCP)/*Internet Protocol* (IP) é a base de todas as comunicações na *Internet*, ele oferece controle de roteamento de informações em uma rede. O protocolo TCP/IP, de acordo com o modelo *Open Systems Interconnection* (OSI), se localizam nas camadas de transporte e de rede respectivamente. Sendo que o HTTP e os demais protocolos de utilização na comunicação de *Web Services* ficam na camada de aplicação (Potss, 2003), como ilustra a figura 8.

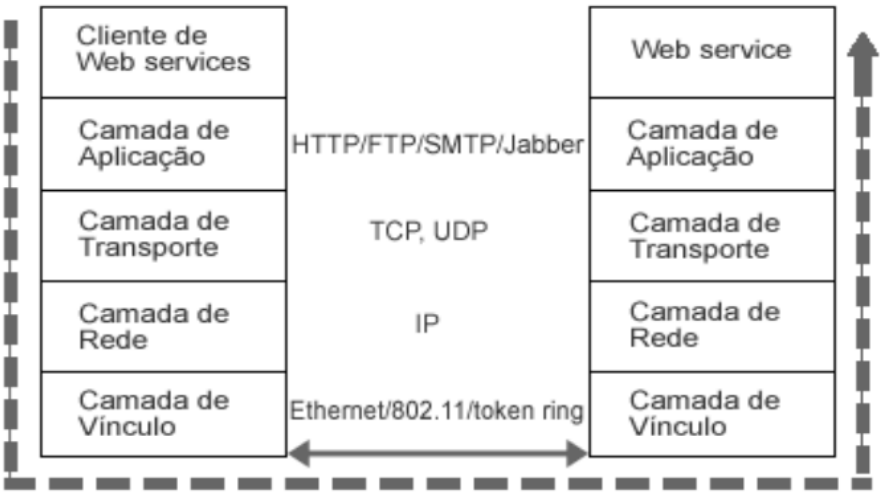

Figura 8. Modelo OSI de Comunicações. (Potss, 2003).

Segundo o RFC 2616 (Fielding *et al*, 1999) o protocolo HTTP é voltado a sistemas distribuídos, colaborativos e hipermídia, tal protocolo está em uso pela WWW desde sua primeira versão (HTTP/0.9), lançada em 1990. Na época, era utilizado para transferir dados brutos através da *Internet*, atualmente está na versão HTTP/1.1. O HTTP tem como base de comunicação a troca de mensagens, ou seja, um cliente envia uma requisição ao servidor, utilizando um método HTTP, uma URI, versão do protocolo, seguida de metadados e podendo possuir um corpo. O servidor responde a solicitação contendo um código de status, podendo ou não apresentar um corpo (Fielding, 2000). Toda a comunicação entre o cliente e o servidor é feita na sequência do *handshake* de comunicação HTTP.

4.1. *Web Services*

Com o desenvolvimento da *Internet*, surgiram novas abordagens ao problema da interoperabilidade entre sistemas de informação, integração entre aplicações, utilização unificada de processos encontrados em diferentes sistemas e escritos em diferentes linguagens. Com o intuito de sanar tais questões, criou-se a tecnologia *Web Services*, permitindo formas de integrar sistemas distintos, modularizar serviços e capacitar à integração e consumo de informações. Notando o avanço de tal tecnologia, os *Web Services* tem chamado a atenção por parte de toda indústria de computadores, a Microsoft, IBM e Sun têm apostado e investido neste conceito ([2]W3C, 2004).

De uma forma sucinta, os *Web Services* procuram facilitar a integração de aplicações distribuídas, tornando possível que aplicações diferentes interajam entre si e sistemas desenvolvidos em plataformas diferentes se tornem compatíveis, permitem que as aplicações enviem e recebam dados em formatos variados, que é traduzida para uma linguagem universal, como é o caso do formato XML ([2]W3C, 2004).

4.1.1. Arquitetura *Representational State Transfer* (REST)

Diante deste contexto, surge a necessidade de disponibilizar serviços de maneira a facilitar sua integração, características estas atendidas por sistemas desenvolvidos utilizando o estilo de arquitetura REST, utilizada para disponibilizar posteriormente o serviço de assinatura digital, formalizado por Roy Fielding em sua tese de doutorado publicado em 2000. REST geralmente é utilizado como modelo para comunicação *Web* (Fielding, 2000).

Segundo Roy (Fielding, 2000), para que os princípios deste modelo sejam respeitados, um conjunto de restrições deve ser seguido:

- Cliente-Servidor: Característica mais comumente encontrada em serviços *Web*. Um servidor, com um ou mais serviços disponíveis, escuta requisições realizadas a tais serviços. Um cliente que deseja a execução do serviço, envia uma requisição para o servidor, o servidor então pode executar ou rejeitar tal serviço, enviando uma resposta ao cliente. Desta maneira é possível melhorar a portabilidade do cliente, através de múltiplas plataformas, e a escalabilidade, permitindo que os componentes possam evoluir independentemente.
- *Stateless* (Sem estado): Tal restrição diz respeito a iteração entre cliente e servidor, cada requisição do cliente deve conter todas as informações necessárias para que seja entendida pelo servidor, deste modo, estados de sessão, quando necessárias, devem ser mantidos no cliente, ou seja, a comunicação deve ser realizada sem o armazenamento de estado no servidor.
- Cache: Exige que os dados de uma resposta, emitida de uma requisição ao servidor, sejam marcadas como *cacheable* ou *noncacheable*, para utilização ou não de *cache*, respectivamente. Com a utilização do *cache* é possível diminuir ou até mesmo eliminar interações com o servidor, otimizando eficiência, escalabilidade e *performance* perante o usuário.
- Interface Uniforme: REST define quatro requisitos de interface: identificação de recursos; manipulação de recursos através de representações; mensagens auto-descritivas e hipermídia como mecanismo de estado de aplicação. Tal característica diferencia a arquitetura REST de outros estilos baseados em rede.

  Atualmente, o HTTP é o protocolo mais indicado para a arquitetura REST, onde provê quatro métodos básicos para as operações: GET – para recuperar uma representação de um recurso; PUT – para criar um novo recurso ou modificar um existente; DELETE – para deletar um recurso e; POST – comumente utilizado para criação de um recurso. A desvantagem na utilização de uma interface uniforme é a diminuição de eficiência, devido os dados serem transmitidos de uma forma padronizada ao invés de serem otimizados de modo as necessidades de uma aplicação específica.
- Multicamada: Sistemas multicamadas utilizam camadas para separar diferentes unidades de funcionalidades, de modo a aperfeiçoar a escalabilidade da *Internet*. A

principal desvantagem de tal modelo está na adição de *overhead* e latência nos dados processados, reduzindo seu desempenho.

- *Code-On-Demand:* Permite a funcionalidade de baixar e executar diretamente o código no lado do cliente. Tal característica é opcional no modelo de arquitetura REST, simplifica a parte do cliente e foca sua extensibilidade, reduzindo a visibilidade.

Nota-se que todos os princípios REST, como protocolo sem estado e *cache* estão presentes na *Web*. Uma característica que não torna um site totalmente REST diz respeito ao conteúdo de resposta/retorno de uma requisição, enquanto o retorno de um serviço REST está voltado à informação, o retorno de uma requisição para um site típico da *Web* é constituído de informações de formatação e estilo para que os dados sejam estruturados para o usuário (Dias *et al*, 2007).

4.2. JavaFX

Em 2005, a Sun Microsystems adquiriu a empresa SeeBeyond, onde o engenheiro de *software* Chris Oliver criou uma linguagem de *script* gráficos ricos, conhecido como F3, mais tarde anunciado pela Sun Microsystems na conferência JavaOne 2007, como JavaFX. Em 20 de abril de 2009, a Oracle Corporation anunciou a aquisição da Sun Microsystems, e novo administrador do JavaFX. No JavaOne 2010, a Oracle anunciou o roteiro JavaFX. Como parte do roteiro, a Oracle revelou seus planos de eliminar progressivamente a linguagem de *script* JavaFX e recriar JavaFX para a linguagem Java e plataforma. Como prometido, baseado no roteiro de 2010, JavaFX 2.0 *Software Development Kit* (SDK) foi lançado no JavaOne 3 de outubro de 2011 (Dea, 2011).

A Oracle também anunciou seu compromisso de tomar medidas para liberar JavaFX como um produto de código aberto, com o propósito de aumentar sua adoção, permitir um rápido tempo de resposta de correções de *bugs*, e gerar novas melhorias. JavaFX é um conjunto de bibliotecas Java projetados para permitir aos desenvolvedores criar e implantar aplicativos "*rich*", que se comportam de forma consistente em todas as plataformas.

Aplicações JavaFX são completamente desenvolvidos em Java, uma das tecnologias mais amplamente implantado com uma das maiores comunidades de desenvolvedores em todo o mundo. JavaFX fornece um rico conjunto de controles de interface do usuário, gráficos

e APIs de mídia com gráficos de alto desempenho com aceleração de *hardware* e motores de mídia para simplificar o desenvolvimento de aplicações imersivas visuais. ([3]ORACLE, 2013), a figura 9 ilustra os componentes da arquitetura da plataforma JavaFX.

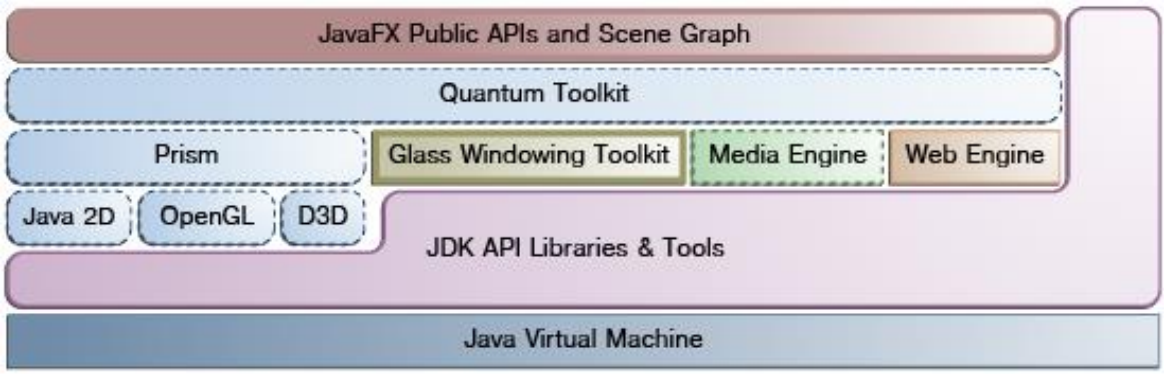

Figura 9. Diagrama da Arquitetura JavaFX. ([1]ORACLE, 2013).

Construir uma aplicação usando o *plugin* JavaFX é um processo relativamente fácil e rápido. É claro que a distância entre um "*Hello, World*!" e uma aplicação realmente útil é muito grande, o que implica em estudar a linguagem mais a fundo e experimentar suas funcionalidades.

JavaFX é o próximo passo na evolução do Java como uma plataforma "*rich client*". Com o JavaFX, os desenvolvedores podem preservar os investimentos existentes, reutilizando bibliotecas Java em suas aplicações. Eles ainda podem acessar os recursos do sistema nativo, ou facilmente conectar a aplicativos de *middleware* baseados em servidor. JavaFX fornece uma plataforma de interface do usuário baseada em Java, capaz de lidar com grandes aplicações de negócios baseadas em dados.

4.2.1. *Rich Internet Application* (RIA)

RIA ou em português, Aplicação de Internet Rica é um tipo de aplicação *Web* cujo objetivo é incrementar e melhorar as opções e capacidades das aplicações tradicionais. O termo RIA foi introduzido pela Macromedia em março de 2002, embora o seu conceito já tenha tido outras denominações anteriores ([1]ORACLE, 2013). Estes novos tipos de aplicações são desenvolvidas, em sua maioria, utilizando linguagens proprietárias. Segundo López, (López, 2005) aplicações RIAs permitem, entre outras coisas, melhorar a experiência de uso da aplicação pelo usuário, execução de conteúdo multimídia e a recuperação de dados da aplicação tanto *online* quanto *offline*, dependendo da tecnologia RIA utilizada.

As aplicações RIAs apresentam algumas vantagens, como menor custo de distribuição, instalação e manutenção, pelo fato da aplicação estar disponível em um servidor *Web*, para que os usuários possam utilizá-la independentemente de local ou sistema operacional. López (López, 2005) destaca outras vantagens:

- Melhorar a experiência visual, com o uso de novos e avançados componentes gráficos;
- Permitir a criação de aplicações mais atrativas ao usuário, mediante a utilização de recursos multimídia de áudio, vídeo e gráficos;
- A maioria das tecnologias RIAs se baseia em linguagem de programação que segue uma formatação similar ao XML, tanto para as interfaces gráficas, como para a transação de dados;
- Os servidores onde executam essas aplicações são bastante variados (.NET, CORBA, *JRun*, *Tomcat*, outros);
- Diminui o consumo de banda utilizado no uso da aplicação, permitindo manejar mais informações de maneira que reduza a quantidade de transações, portanto, também reduz o consumo de memória no servidor onde a aplicação está hospedada;
- O modelo de requisição e resposta não é necessário para cada ação realizada na interface de usuário. Com as aplicações RIAs o usuário interage com a interface de usuário e a aplicação se comunica com o servidor somente quando for necessário;
- Requer a utilização de um "*rich client*" no lado do usuário, que será o motor da tecnologia RIA utilizada (normalmente é um *plugin* no *browser* do usuário);
- Visualização e execução da aplicação RIAs em múltiplas plataformas e dispositivos de *hardware* distintos;
- Possibilita a detecção de eventos da maioria dos componentes e a atualização dos mesmos sem a necessidade de realizar um *refresh* da janela do *browser*;
- Permite realizar funcionalidades como o *drag & drop*, redimensionamento de objeto e outros eventos de interface mais elaborados;
- A transição entre os estado da aplicação se realiza por objetos.

Na prática, aplicações que envolvem o conceito RIA são aplicações *Web* que contém

características e funcionalidades de aplicações *Desktop*, tais aplicações transferem todo o processamento da interface para o navegador da *Internet*, porém mantém a maior parte dos dados, como estado do programa e banco de dados, no servidor da aplicação. RIA não surge com o propósito de substituir aplicações *Desktop*, mas complementá-las. A figura 10 ilustra tal intersecção.

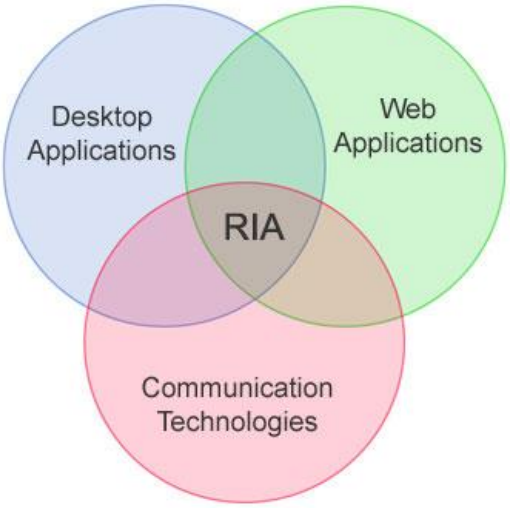

Figura 10. Modelo de Iteração RIA. (Adaptado López, 2005).

4.3. Serviço de Assinatura Digital ICP-Brasil

Os *Web Services* são classificados como um tipo específico de serviço, o qual é identificado com URI, estes são independentes de linguagens de programação, sistemas operacionais e arquiteturas. Com o uso de padrões abertos, como o XML e o HTTP, com os *Web Services* é possível garantir a interoperabilidade entre clientes e provedores de serviços, sem que os mesmos necessitem possuir conhecimento prévio de quais tecnologias estão presentes em cada lado, como visto anteriormente.

A arquitetura REST utilizada para comunicação cliente/servidor, apresenta, entre outras, a característica de *code-on-demand*, permitindo que o cliente possa baixar e executar localmente o código, simplificando aos clientes reduzir o número de recursos requeridos para ser pré-aplicado. O estudo da tecnologia JavaFX possibilitou o aprendizado do conceito RIA, onde possibilita que aplicações que tenham características de *software Desktop* rodem na *Web*.

Com a tendência de muitos serviços estarem migrando para o conceito de *Web Service*, devido ao ambiente *Web* ter se tornado o principal canal de comunicação e relacionamento de

informações, surgiu a oportunidade de implementar o Assinador ICP-Brasil como um serviço, desta maneira o usuário munido do seu certificado digital realiza uma requisição ao servidor e a API do Assinador ICP-Brasil é carregado no *browser* do cliente, para que o serviço seja consumido pelo cliente localmente, onde é realizada a assinatura digital do documento eletrônico. A figura 11 representa o esquema da assinatura digital disponibilizada como um serviço.

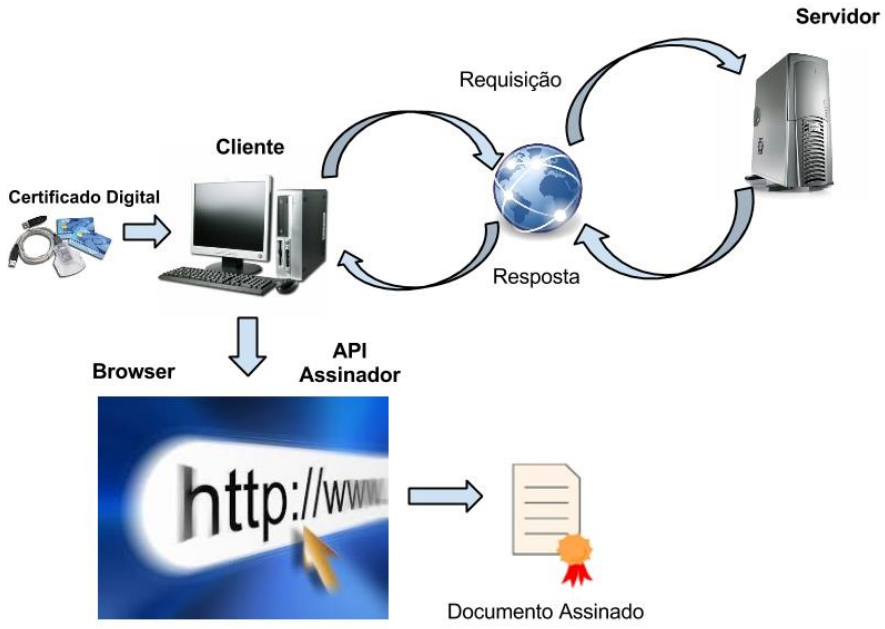

Figura 11. Esquema do Serviço de Assinatura Digital. (Própria).

Para que documentos eletrônicos sejam assinados digitalmente é necessário que a aplicação possa reconhecer e gerenciar os certificados digitais do usuário. Tais certificados, tanto os instalados na máquina quanto os mantidos em um *token*, ficam armazenados em um repositório local para que sejam consumidos por aplicações com tal finalidade. Vale ressaltar que a API Assinador Digital ICP-Brasil foi desenvolvido para o sistema operacional *Windows*, portanto, acessa o *keystore* do *Windows* onde os certificados são armazenados, através do código demostrado na figura 12.

```
KeyStore keyStore = KeyStore.getInstance("Windows-MY", "SunMSCAPI");
```

Figura 12. Código de Acesso ao *keystore* do *Windows*. (Própria).

Para o gerenciamento dos certificados digitais foi implementado o método “certificates”, em JavaFX, utilizando a API Assinador Digital ICP-Brasil, de modo que sejam

carregados todos os certificados contido no repositório específico. São armazenados em uma lista e mostrados ao usuário, para escolha do certificado a ser utilizado para realizar a assinatura digital, como ilustrado na figura 13. Importante ressaltar que os certificados selecionados são somente os de usuários finais, utilizados para a assinatura digital, outros certificados digitais e certificados de ACs não são selecionados e mostrados ao usuário.

```
...
Label lblLista = new Label("Certificado Digital");
lblLista.setUnderline(true);
ListView<String> list = new ListView<String>();
ObservableList<String> items = null;

try {
    int index = 0;
    while(certificate != null){
        items = FXCollections.observableArrayList (certificates(index));
        index ++;
    }
} catch (KeyStoreException ex) {
    Logger.getLogger(Novo.class.getName()).log(Level.SEVERE, null, ex);
}
list.setItems(items);
...
private String certificates(int index) throws KeyStoreException{
    certificate = ICPBrasilStore.getInstance().getSigners().get(index);
    return certificate.getAlias();
}
```


Figura 13. Código para o Gerenciamento de Certificados. (Própria).

Com o certificado digital escolhido pelo usuário para realizar a assinatura digital, é necessário selecionar o documento a ser assinado. Para isso o usuário seleciona um arquivo de sua máquina. Foi usado a API do Java "*JFileChooser*", que fornece uma interface gráfica para navegar no sistema de arquivos, e em seguida, escolher um arquivo ou pasta a partir de uma lista ou digitando o nome de um arquivo ou diretório. Para testes simples, foram escolhidos somente arquivos com extensão .txt, ilustrado na figura 14.

```
...
final TextField inputOpen = new TextField("Busca Arquivo");
inputOpen.setPrefWidth(200);

final FileChooser fileChooser = new FileChooser();

FileChooser.ExtensionFilter extentionFilter = new
        FileChooser.ExtensionFilter("DOC files (*.txt)", "*.txt");
fileChooser.getExtensionFilters().add(extentionFilter);

final Button inputOpenButton = new Button("Buscar");

inputOpenButton.setOnAction(
        new EventHandler<ActionEvent>() {
    @Override
    public void handle(final ActionEvent e) {
        file = fileChooser.showOpenDialog(stage);
        if (file != null) {
            inputOpen.setText(file.getName());
        }
    }
});
...
```

cria FileChooser

extensão .txt

ação do Button de busca, com retorno do nome do arquivo selecionado

Figura 14. Código para Busca de Arquivo. (Própria).

Para a assinatura de documentos eletrônicos, foi implementado o método “digitalsign”, em JavaFX, utilizando a API Assinador Digital ICP-Brasil. Com o certificado digital e o arquivo que se deseja assinar selecionados, estes são passados por parâmetro para o método, de modo a realizar a assinatura digital. O método implementado realiza assinatura digital no formato AD-RB, estabelecido pela ICP-Brasil, como mostra a figura 15.

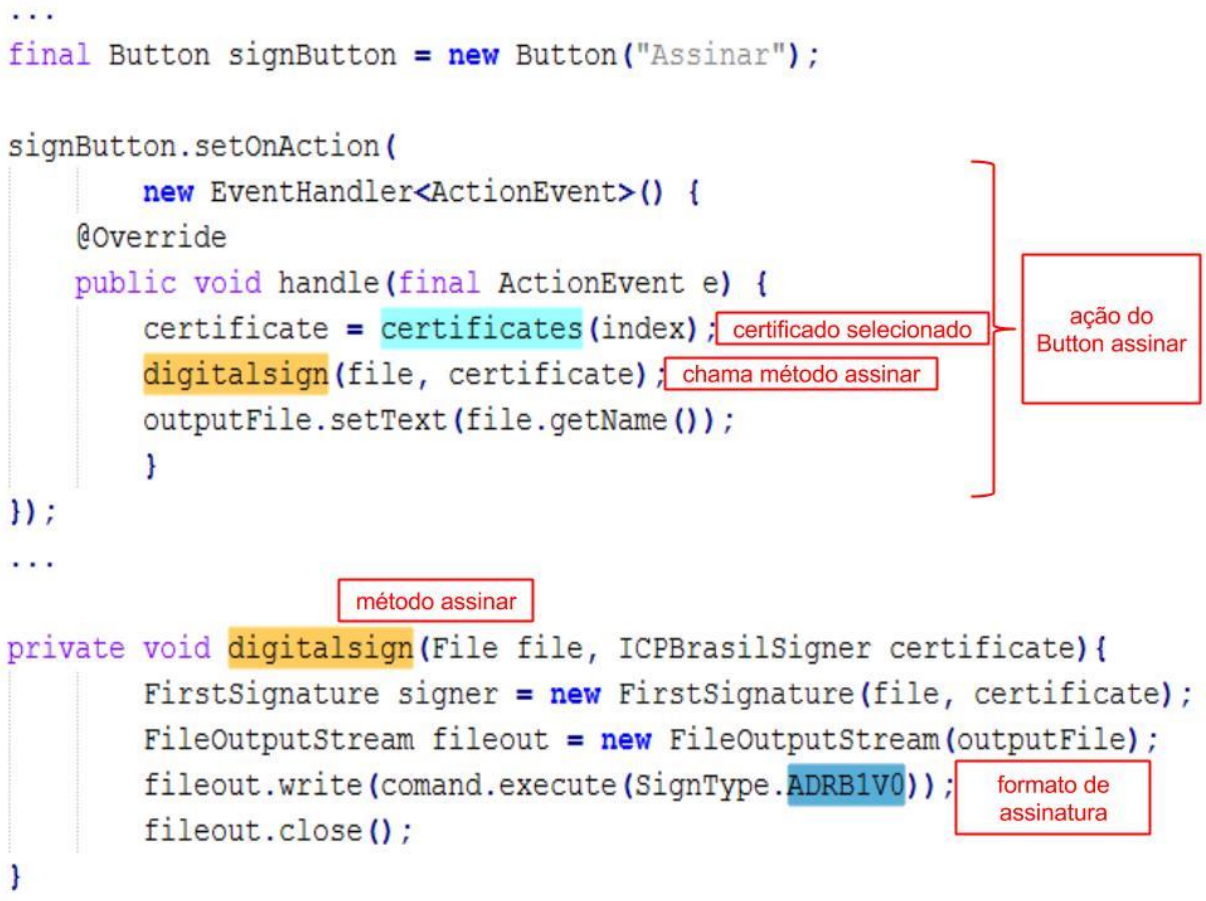

Figura 15. Código para Assinatura Digital. (Própria).

Para disponibilizar a aplicação desenvolvida em uma página *Web*, foi criado um projeto Java *Web*, no próprio NetBeans, como mostra a figura 16, e para este foi criado uma pasta “Assinador” e copiado todos os arquivos da pasta “dist” gerados ao compilar a aplicação desenvolvida em JavaFX, além das pastas “lib” e “web-files”, os arquivos .html destacado em roxo e os arquivos .jar e .jnlp destacados em verde, desta forma a aplicação pode ser consumida na página *Web*. Nota-se que todas as APIs utilizadas no desenvolvimento do assinador, inclusive a API Assinador Digital ICP-Brasil, também constam no projeto *Web*.

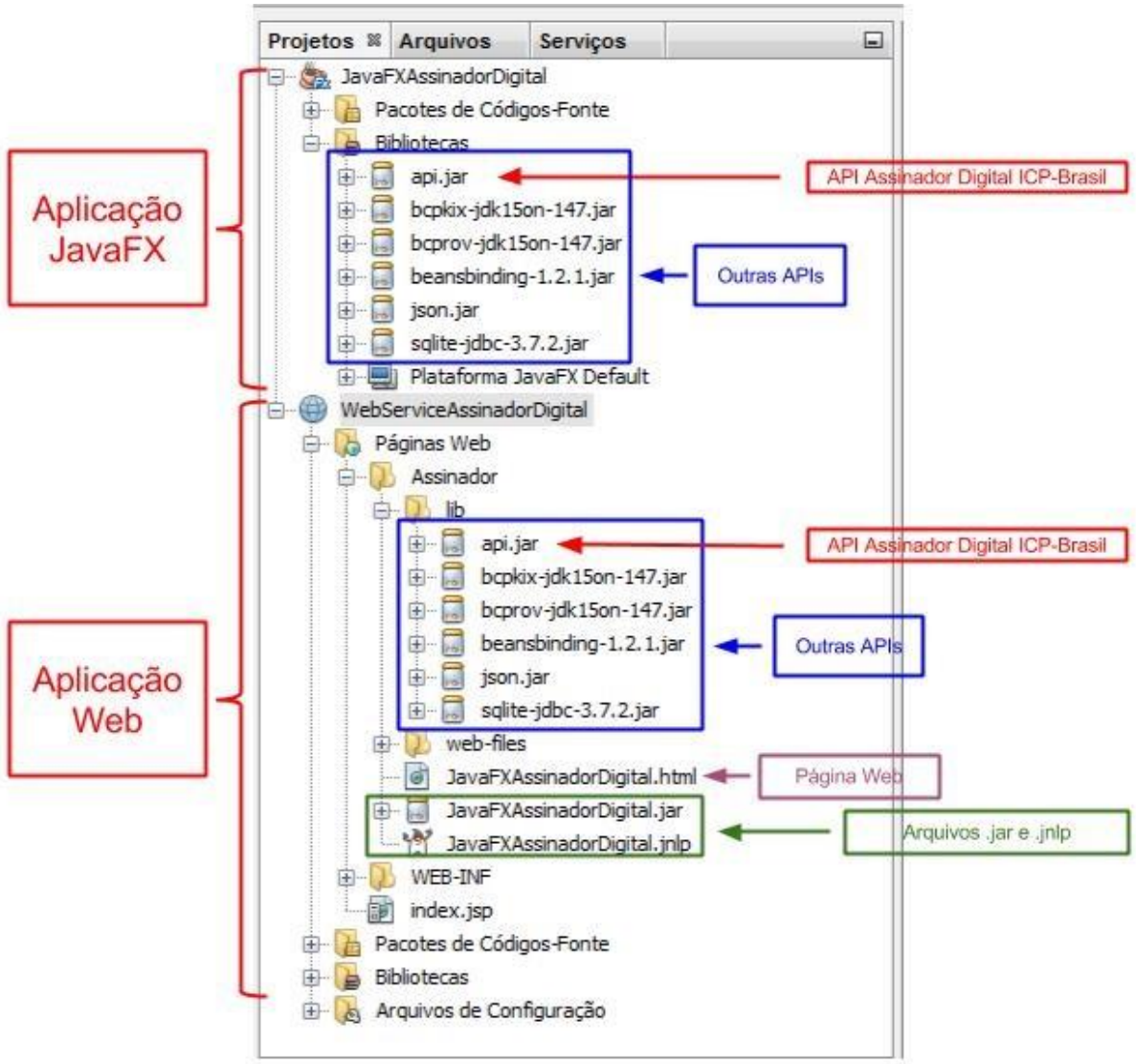

Figura 16. Projeto *Web* Assinador Digital. (Própria).

4.3.1. Testes

O primeiro teste realizado na aplicação desenvolvida verifica sua capacidade de acessar o *keystore* do *Windows*, de modo que possa gerenciar os certificados contidos em seu repositório. Tal teste teve seu resultado esperado, mostrando os certificados em uma lista para que o usuário selecione o desejado, como mostra a figura 17.

Figura 17. Lista de Certificados. (Própria).

Ponto importante neste teste, foi a necessidade de assinar o arquivo .jar gerado. Isto é necessário devido à aplicação ser carregada no *browser* e acessar arquivos privados do cliente. O NetBeans possui a funcionalidade de gerar arquivos auto assinados, tal funcionalidade foi utilizada por não possuir um certificado específico para realização da assinatura. Deste modo foi possível a continuação do desenvolvimento e testes da aplicação.

O segundo teste realizado foi referente à assinatura digital gerada. Este também teve seu resultado esperado, como mostra a figura 18. Devido a API Assinador Digital ICP-Brasil realizar assinaturas nos formatos e especificações estabelecidas pela ICP-Brasil, de modo que constam no CMS os atributos assinados e não assinados. Utilizou-se o *software* ViewBer, por ser um utilitário gratuito que exibe a estrutura ASN.1 de um arquivo codificado em BER. ViewBer pode ser usado para exibir o conteúdo de certificados X509 codificados em DER e PEM, PKCS # 12, PKCS # 10, arquivos de RSE, PKCS # 7, entre outros.

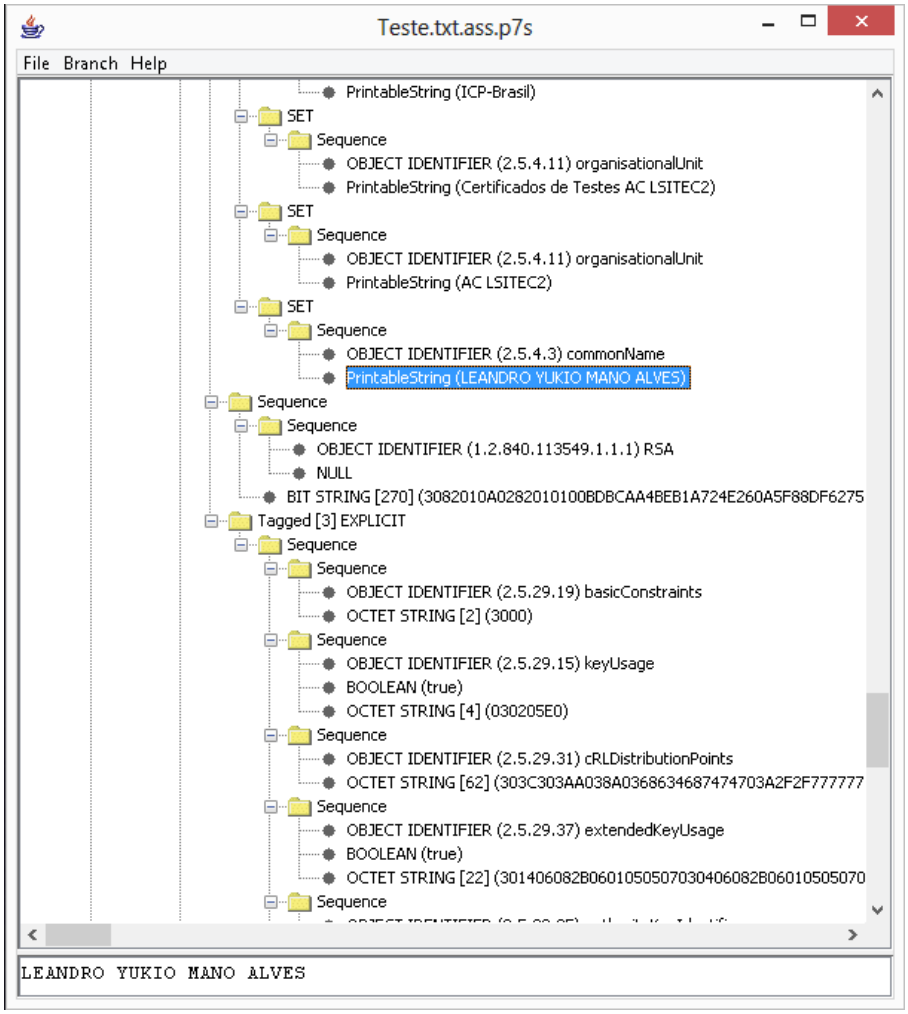

Figura 18. Estrutura da Assinatura Digital Gerada. (Própria).

Por fim, verificou a aplicação disponibilizada como um serviço. Para tal teste foi utilizado o servidor GlassFish Server 4.0, que consta integrado no NetBeans 7.3.1, e teve seu resultado esperado. A aplicação é carregada completamente no *browser* do cliente, através do método GET, como mostra a figura 19, e esta realiza toda a operação de assinatura digital do documento eletrônico sem a necessidade de realizar requisições ao servidor, garantindo que a chave privada do usuário não seja transporta pela rede.

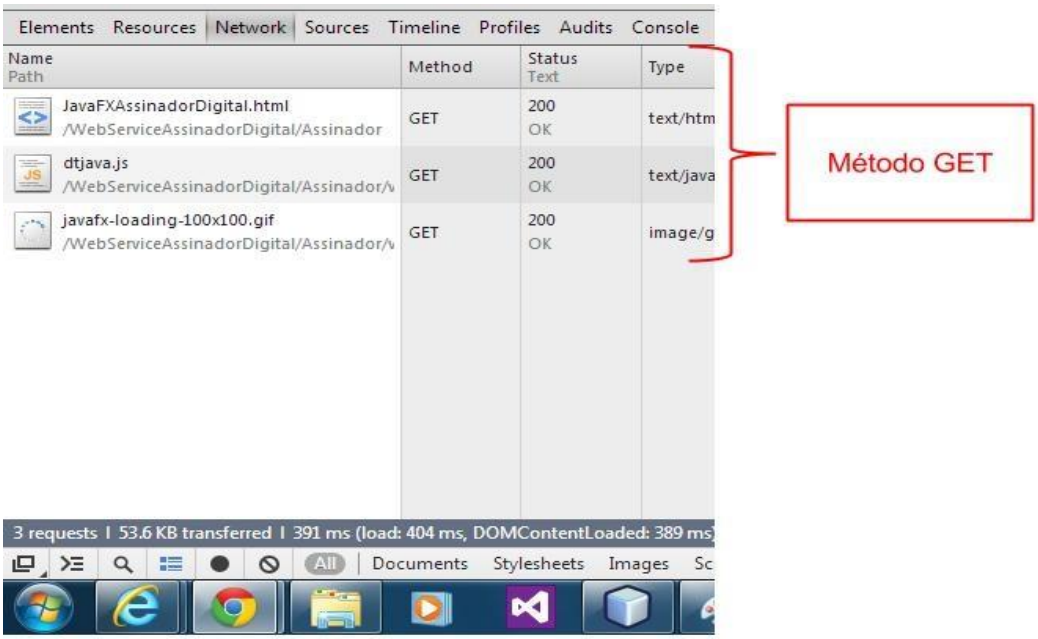

Figura 19. Teste 1 do método GET. (Própria).

Para um teste mais específico, foi utilizada a ferramenta Dev HTTP Client, que permite aos desenvolvedores realizar testes de recursos HTTP/HTTPS. A figura 20 mostra, destacados, o endereço da aplicação, o método utilizado e o status da resposta, verificando que através do método GET obteve o resultado esperado.

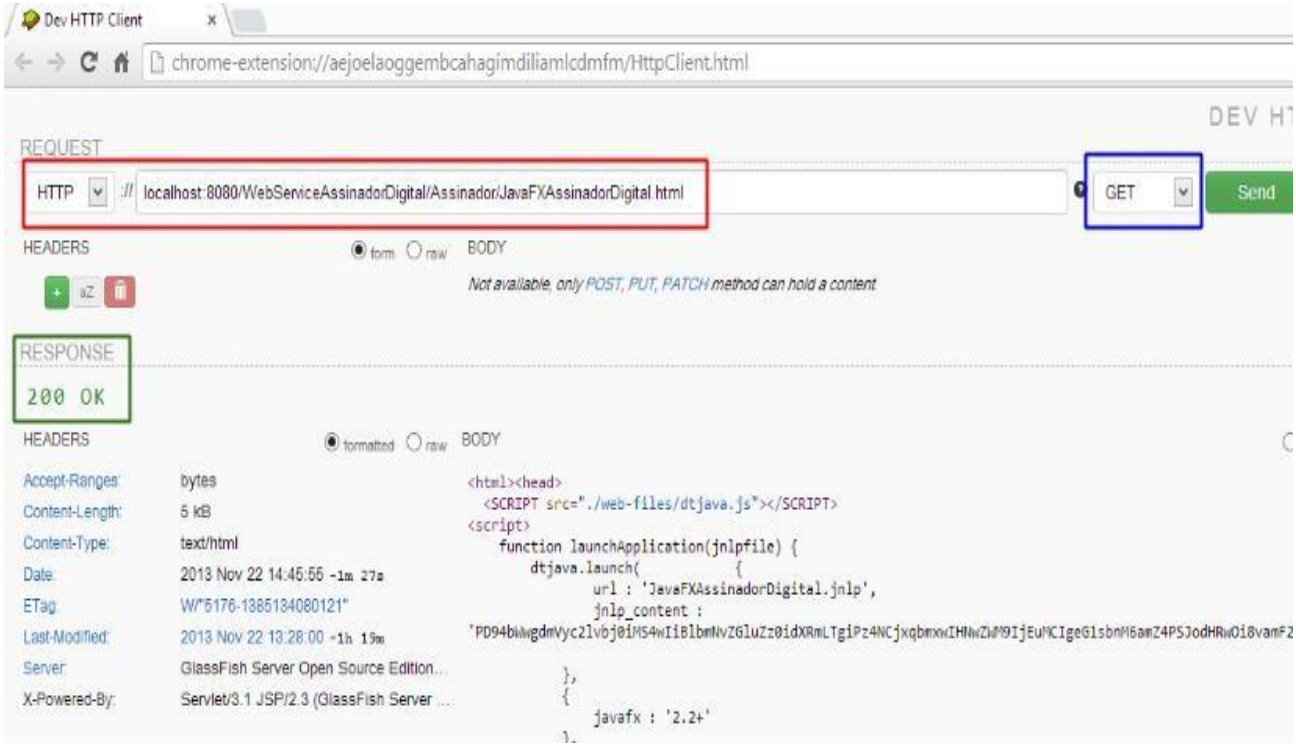

Figura 20. Teste 2 do método GET. (Própria).

O mesmo teste mostra, como resposta, o código utilizado para o carregamento do arquivo *Java Network Launching Protocol* (JNLP). Ao compilar o projeto em JavaFX é gerado em sua pasta “dist” o arquivo JavaFXAssinadorDigital.jnlp, que por sua vez é copiado ao projeto *Java Web*, como descrito anteriormente. Desta maneira, levando em conta como está descrito na página HTML, o arquivo .jnlp é lançado automaticamente, realizando o *download* da aplicação para a máquina do usuário, mostrado na figura 21.

Figura 21. Resposta do Método GET. (Própria).

Arquivos .jnlp é definida como um XML *schema*, que consiste de um conjunto de regras que definem como implantar o mecanismo para lançar aplicações *Java Web Start*. Arquivos JNLP possuem informações como a localização do arquivo .jar, arquivo de pacote, nome da classe principal, entre outros parâmetros. O navegador passa o arquivo JNLP a um JRE, que por sua vez realiza o *download* do aplicativo na máquina do usuário e inicia sua execução ([4]ORACLE, 2013). A figura 22 mostra uma parte do arquivo JavaFXAssinadorDigital.jnlp, destacando os *downloads* realizados dos arquivos .jar.

```
<?xml version="1.0" encoding="utf-8"?>
<jnlp spec="1.0" xmlns:jfx="http://javafx.com" href="JavaFXAssinadorDigital.jnlp">
  <information>
    <title>JavaFXAssinadorDigital</title>
    <vendor>Leandro</vendor>
    <description>Sample JavaFX 2.0 application.</description>
    <offline-allowed/>
  </information>
  <resources>
    <jfx:javafx-runtime version="2.2+" href="http://javadl.sun.com/webapps/download/GetFile/javafx-lates
  </resources>
  <resources>
    <j2se version="1.6+" href="http://java.sun.com/products/autodl/j2se"/>
    <jar href="JavaFXAssinadorDigital.jar" size="20857" download="eager" />
    <jar href="lib/api.jar" size="368691" download="eager" />
    <jar href="lib/bcpkix-jdk15on-147.jar" size="515071" download="eager" />
    <jar href="lib/bcprov-jdk15on-147.jar" size="1997327" download="eager" />
    <jar href="lib/beansbinding-1.2.1.jar" size="282189" download="eager" />
    <jar href="lib/json.jar" size="37875" download="eager" />
    <jar href="lib/sqlite-jdbc-3.7.2.jar" size="3201133" download="eager" />
  </resources>
  <applet-desc  width="800" height="600" main-class="com.javafx.main.NoJavaFXFallback"  name="JavaFXAssi
    <param name="requiredFXVersion" value="2.2+"/>
  </applet-desc>
```

JavaFXAssinadorDigital.jar

Figura 22. Arquivo JavaFXAssinadorDigital.jnlp. (Própria).

RESULTADOS

Com o estudo da linguagem JavaFX foi implementado uma interface, de modo que possa realizar a assinatura digital de documentos eletrônicos, ilustrada na figura 23. A interface implementada dispõe das funcionalidades:

- Opção de Assinatura: apresenta ao usuário opções de diferentes processos para geração da assinatura digital: a) Realizar Primeira Assinatura Digital; b) Adicionar Assinatura Digital (Co-Assinatura), permite que vários usuários assinem o mesmo documento eletrônico; c) Redefinir Formato de Assinatura, permite o usuário migrar entre os formatos de assinaturas digitais e; d) Adicionar Assinatura Digital, permite ao usuário adicionar sua assinatura em um documento assinado;
- Formato de Assinatura: apresenta todos os formatos disponíveis de assinaturas digitais, estes estabelecidos pela ICP-Brasil (AD-RB, AD-RT, AD-RV, AD-RC e AD-RA);
- Busca Arquivo de Entrada: permite ao usuário escolher, de maneira fácil e transparente, o arquivo que deseja assinar digitalmente;
- Lista de Certificados: apresenta os certificados que podem ser utilizados para realizar assinaturas digitais de documentos eletrônicos, deste modo o usuário escolhe o certificado que deseja utilizar;
- Gera Arquivo de Saída: permite ao usuário escolher o nome do novo arquivo gerado, este assinado;
- Assinar: após todas as opções selecionadas de acordo com a escolha do usuário, este utiliza todos os parâmetros fornecidos e com o auxílio da API Assinador Digital ICP-Brasil realiza a assinatura do documento.

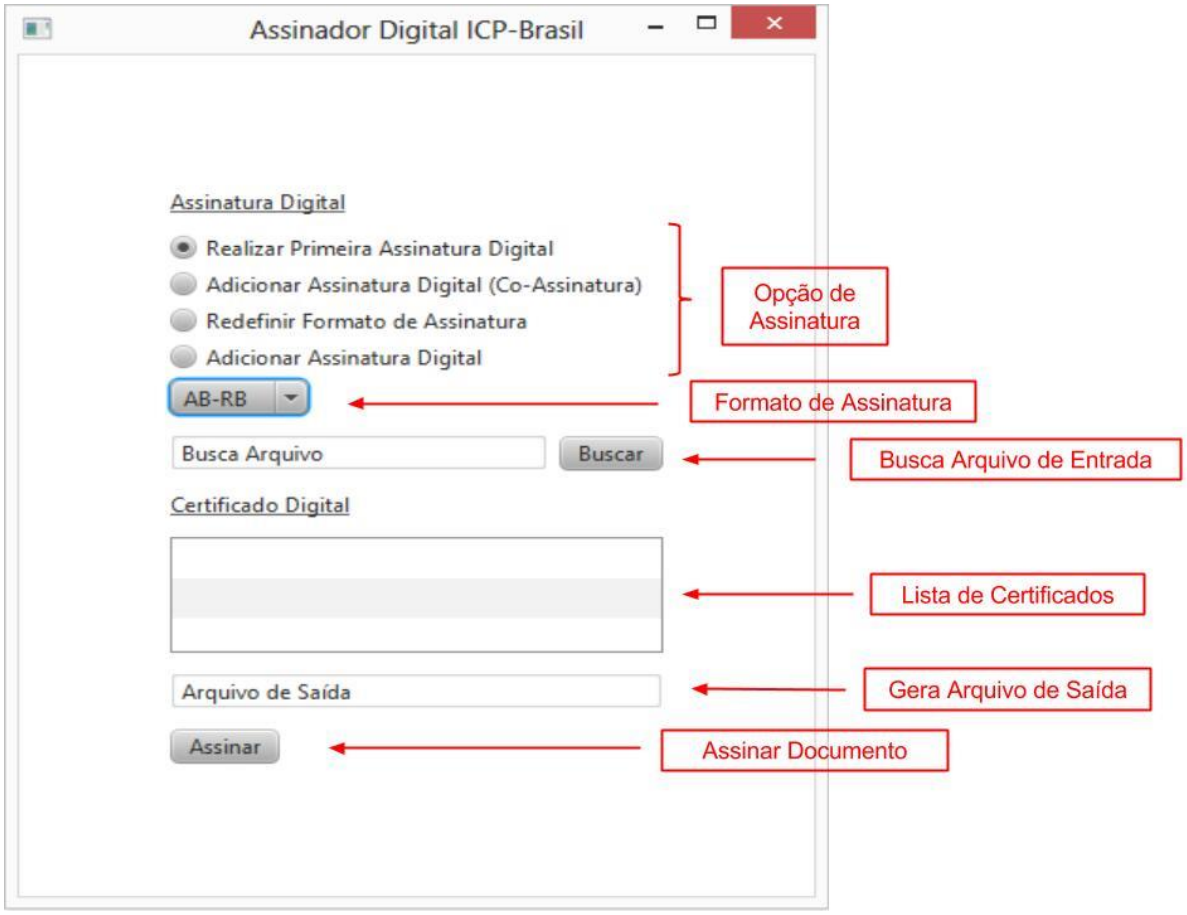

Figura 23. Assinador Digital ICP-Brasil, Implementação em JavaFX. (Própria).

Com os estudos realizados sobre *Web Service* e arquitetura REST, foi possível disponibilizar a aplicação desenvolvida em JavaFX, com todas as funcionalidades implementadas descritas acima, com o apoio da API Assinador Digital ICP-Brasil, para que seja consumida como um serviço através da *Internet*, de modo a garantir a segurança e validade de todo processo de geração da assinatura digital de documentos eletrônicos. A figura 24 mostra o Assinador Digital ICP-Brasil disponibilizado como um serviço.

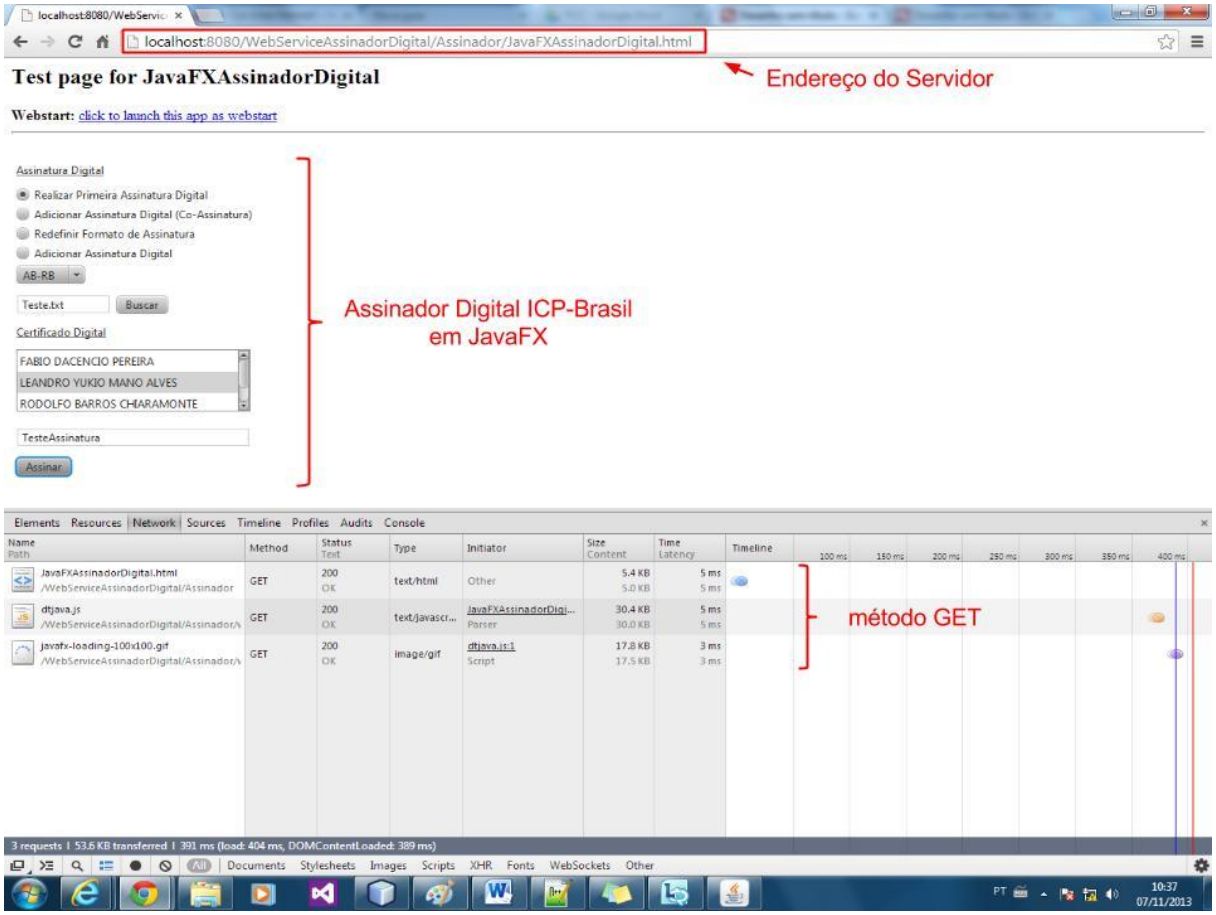

Figura 24. Serviço de Assinatura Digital ICP-Brasil via *Web*. (Própria).

CONCLUSÕES

Destacou-se que a ICP-Brasil estabelece requisitos mínimos para geração e verificação de assinaturas digitais, previstos e descritos em documentos por ela emitidos. O estudo da infraestrutura da ICP-Brasil revelou que não há objeção à adoção de software de especialidade que permita a co-assinatura digital e assinaturas em lote, desde que obedeça aos padrões e critérios de validade jurídica do documento eletrônico por ela estabelecidos.

Em algumas operações eletrônicas assinadas digitalmente, o uso de carimbo de tempo é uma forma confiável de agregar e registrar a data e o horário das transações de documentos eletrônicos. A adoção da certificação do carimbo de tempo, portanto, permite obter prova que tal documento assinado existia, assim como o certificado digital nele empregado, na data incluída no carimbo de tempo, maximizando a segurança jurídica no processo de certificação digital e tramitação do documento eletrônico.

Assim, o Assinador Digital ICP-Brasil, desenvolvido em parceria do LSI-TEC e o COMPSI, segue todos os processos de geração de assinaturas válidas estabelecidos pela ICP-Brasil, de modo a garantir a integridade, autenticidade e não-repúdio dos documentos eletrônicos.

O presente trabalho visou à implementação de um serviço de assinatura digital, que tinha por finalidade, entre outras coisas, disponibilizar um serviço via *Web* de assinatura digital seguindo as normas de segurança estabelecidas pela ICP-Brasil. Tal objetivo foi atingido através do estudo e utilização da tecnologia JavaFX e a API Assinador Digital ICP-Brasil.

Conclui-se que disponibilizar um serviço de assinatura digital via *Web* pode facilitar a adoção de tal tecnologia perante a sociedade, de modo que documentos eletrônicos possam ser assinados e transportados de forma segura, garantindo sua validade jurídica.

Como trabalho futuro, sugere-se disponibilizar o Serviço de Assinatura Digital ICP-Brasil, utilizando a arquitetura REST para um ambiente real, para que testes de desempenho e segurança possam ser analisados e melhorados.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, L. Y. M.; Guelfi, A. E.; Pereira, F. D.; Chiaramonte, R. B.; Tognoli, E. L. e Teotonio, C. A. (2012). Assinador Digital ICP-Brasil: Implementação de Referência em Java. In: 10º CertForum, 2012, Florianópolis, 2012.

ALVES, L. Y. M.; Pereira, F. D., Neto, M. F. e Nascimento, B. (2013). A Petição Eletrônica: Co-Assinatura Digital e a Importância de Requisitos Temporais. In: 2º CONGRESO IBEROAMERICANO DE INVESTIGADORES Y DOCENTES DE DERECHO E INFORMÁTICA - CIIDDI, Florianópolis, 2013.

BERNERS-LEE, Tim; FIELDING, Roy Thomas; W3C; UC Irvine; J. Gettys; L. Masinter; Xerox. Uniform Resource Identifier (URI): Generic Syntax, 1998. Disponível em: < http://tools.ietf.org/html/rfc2396 >. Acesso em: 12 de Outubro de 2013.

CAIXA (2013). Caixa: primeira Autoridade Certificadora do Tempo da ICP-Brasil. Disponível em: < http://www.iti.gov.br/noticias/boletim-digital/4171-boletim-digital-273 >. Acesso em: 01 de Março de 2013.

CUSTÓDIO, Ricardo Felipe. Análise crítica da ICP-Brasil: resposta à consulta pública. Florianópolis: Laboratório de Segurança da Computação/UFSC, 2001. 18p.

DEA, Carl P. JavaFX 2.0: Introduction by Example. New York: Apress, 2011. xiii

Decreto nº 3.587, de 5 de setembro de 2000. Estabelece normas para a Infraestrutura de chaves públicas do Poder Executivo Federal – ICP-Gov. E dá outras providências. Disponível em: < http://www.senado.gov.br/legislacao/ >. Acesso em: 26 de Fevereiro de 2013.

Decreto nº 3.996, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da administração pública federal. Disponível em: < http://www.senado.gov.br >. Acesso em: 28 de Fevereiro de 2013.

Decreto nº 4.414, de 7 de outubro de 2002. Altera o Decreto 3.996, de 31 de outubro de 2001, que dispõe sobre a prestação de serviços de certificação digital no âmbito da administração pública federal. Disponível em: < http://www.senado.gov.br >. Acesso em: 28 de Fevereiro de 2013.

DEVEGILI, Augusto Jun. Farnel: uma proposta de protocolo criptográfico para votação digital. Dissertação (Mestrado em Ciência da Computação) - Faculdade de Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2001. Disponível em: < http://www.labsec.ufsc.br >. Acesso em: 20 de Dezembro de 2012.

DIAS, Ari Neto; MACHADO, Lucas Alves. REST com Struts 2. Java Magazine, São Paulo, Edição 48, pág. 58 a 66, 2007.

FIELDING, Roy Thomas. Architectural Styles and the Design of Network – based Software Architectures. 200. Tese (Doutorado em Informação e Ciência da Computação) – Universidade da Califórnia, Califórnia, 2000.

FIELDING, Roy Thomas; BERNERS-LEE, Tim; W3C; UC Irvine; J. Gettys; Compaq; H. Frystyk; J. Mogul; L. Masinter; Xerox; Microsoft; P. Leach. Hypertext Transfer Protocol -- HTTP/1.1, 1999. Disponível em: < ftp://ftp.isi.edu/in-notes/rfc2616.txt >. Acesso em: 02 de outubro de 2013.

FREITAS, Vinicius Pimentel; LOEBENS, João Carlos. Contratos eletrônicos e o comércio internacional: uma proposta. 2004. Disponível em: < http://www.inap.map.es >. Acesso em: 30 de Novembro de 2012.

GUIMARÃES, José Augusto Chaves; NASCIMENTO, Lúcia Maria Barbosa; FURLANETO NETO, Mário. Aspectos jurídicos e diplomáticos dos documentos eletrônicos. São Paulo: Associação de Arquivistas de São Paulo, 2005. 74p.

ICP-Brasil, (2009). Requisitos Mínimos para as Declarações de Práticas das Autoridades de Carimbo de Tempo da ICP-Brasil – DOC-ICP-12 – Versão 1.1. Brasil.

ICP-Brasil, (2012). Requisitos para Geração e Verificação de Assinaturas Digitais na ICP-Brasil – DOC-ICP-15.01 – Versão 2.1. Brasil.

ICP-Brasil, (2010). Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil – DOC-ICP-11 – Versão 1.2. Brasil.

ITI, (2013). Instituto Nacional de Tecnologia da Informação (ITI). Estrutura da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Disponível em: < http://www.iti.gov.br/icp-brasil >. Acesso em: 14 de Março de 2013.

LÓPEZ, Xavier Farré. Trabalho de conclusão de curso: Rich Internet Application. Universidade Politécnica da Catalunia, Espanha, 2005. Disponível: < http://upcommons.upc.edu/pfc/bitstream/2099.1/3720/4/40624-4.pdf >. Acesso em 13 de Setembro de 2013.

Media Provisória 2.200/2, de 24 de outubro de 2011. Institui a Infraestrutura de chaves públicas brasileira – ICP-Brasil, transforma o instituto nacional de tecnologia da informação em autarquia, e dá outras providências. Disponível em: < http://www.senado.gov.br/legislacao/ >. Acesso em: 26 de Fevereiro de 2013.

[1]ORACLE, (2013). JavaFX Documentation Home > JavaFX Overview. Disponível em: < http://docs.oracle.com/javafx/2/overview/jfxpub-overview.htm >. Acesso em: 12 de Maio de 2013.

[2]ORACLE, (2013) “NetBeans IDE 7.3 Release Information”. Disponível em: < https://netbeans.org/community/releases/73/ >. Acesso em: 15 de Maio de 2013.

[3]ORACLE, (2013). Oracle Technology Network > Java > JavaFX > Overview. Disponível em: < http://www.oracle.com/technetwork/java/javafx/overview/index.html >. Acesso em: 25 de Novembro de 2013.

[4]ORACLE, (2013). JNLP File Syntax. Disponível em < http://docs.oracle.com/javase/1.5.0/docs/guide/javaws/developersguide/syntax.html >. Acesso

em 02 de Dezembro de 2013.

POTSS, Stephen (2003). Aprenda Web Services em 24 Horas: Para quem não pode perder tempo 24 lições de 1 hora. Editora Elsevier, 2003.

RAMOS, Ruy (2013). Certificado de Atributo na ICP-Brasil. Disponível em: < http://www.iti.gov.br/noticias/indice-de-noticias/4267-artigo-certificado-de-atributo-na-icp-brasil >. Acesso em: 15 de Maio de 2013.

Resolução Nº 41, de 18 de Abril de 2006. Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil. Disponível em < http://www.iti.gov.br/images/icp-brasil/legislacao/Resolucoes/RESOLU__O_41_DE_18_04_2006.PDF >. Acesso em: 25 de Maio de 2013.

SIGN SERVER. Disponível em < signserver.org >. Acessado em: 17 de Setembro de 2012.

STALLINGS, Willian. Criptografia e segurança de redes. São Paulo: Pearson, 2008. 492p.

VOLPI, Marlon Marcelo. Assinatura digital - aspectos técnicos, práticos e legais. Rio de Janeiro: Axcel Books, 2001. 121p.

[1]W3C, (2004). Architecture of the World Wide Web, Volume One. Disponível em: < http://norman.walsh.name/2004/12/15/examples/webarch.pdf >. Acesso em: 04 ago. 2009.

[2]W3C, (2004). Web Services Architecture: W3C Working Group. Disponível em: < http://www.w3.org/TR/ws-arch/ >. Acesso em: 15 de Agosto de 2013.