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

ASSINADOR DIGITAL ICP – BRASIL: PLUGIN PARA NAVEGADORES WEB

MARCOS HENRIQUE DE OLIVEIRA

Marília
2015

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

ASSINADOR DIGITAL ICP – BRASIL: PLUGIN PARA NAVEGADORES 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
2015

DEDICATÓRIA

Dedico primeiramente a Deus por ter concedido a mim total capacidade, força e inteligência para realização deste trabalho tão importante nesta etapa de minha vida.

Dedico este trabalho as minhas mães, Angela Maria da Silva e Creuza Maria dos Santos Silva (Avó) que mesmo não entendendo muito sobre o meu curso sempre me apoiaram em momentos de dificuldades.

Ao meu Irmão Natan da Silva Wenceslau que mesmo sem compreender, foi uma motivação indescritível para que conseguisse alcançar tal objetivo.

AGRADECIMENTOS

Primeiramente a Deus por ter me dado saúde e força para superar as dificuldades permitindo que tudo isso acontecesse ao longo de minha vida, e não somente nestes anos como universitário, mas que em todos os momentos é o maior mestre que alguém pode conhecer.

Agradeço ao meu orientador, Prof. Dr. Fábio Dacêncio Pereira, pela oportunidade, apoio e incentivo na elaboração deste trabalho e por ser um excelente professor e profissional, o qual me espelho.

A esta universidade, seu corpo docente, direção e administração pela oportunidade de Ingressar nessa Universidade com bolsa 100% em todos os Anos da graduação.

As minhas Mães Angela da Silva e Creuza Maria (avó) heroínas que me deram apoio incondicional, amor e incentivo nas horas difíceis, de desânimo e cansaço.

Agradeço também a minha namorada, Ellen Colombo, que de forma especial e carinhosa me deu força e coragem, me apoiando nos momentos de dificuldade.

Agradeço ao Prof. Ricardo José Sabatine que com muita humildade me ajudou em alguns momentos de dificuldades nesta etapa final do projeto.

Como não poderia esquecer de Agradecer aos meus amigos Alecsandre Porto , Gabriel Pavanello e Danilo Maciel companheiros de faculdade e irmãos na amizade que fizeram parte da minha formação e que vão continuar presentes em minha vida com certeza.

Em especial ao Danilo Maciel, que com muita humildade e simplicidade, me ajudou em vários momentos de dificuldades.

Ao meu Amigo Luiz Felipe pela paciência em ler por diversas vezes a minha monografia.

Por isso lutar, conquistar, vencer e até mesmo cair e perder, e o principal, viver é o meu modo de agradecer sempre.

E a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AC - Autoridade Certificadora

AC - Raiz - Autoridade Certificadora Raiz

ACT - Autoridade Certificadora do Tempo

API - *Application Programming Interface*

DPC - Declaração de Práticas de Certificação

AR – Autoridades de Registros

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

DES - *Data Encryption Standard*

EAS - *Advanced Encryption Standard*

HTML - *HyperText Markup Language*

ICANN - Internet para Atribuição de Nomes e Números

ICP - Brasil - Infraestrutura de Chaves Públicas Brasileira

IDEA - *International Data Encryption Algorithm*

IDE - *Integrated Development Environmen*

IEC - *International Electrotechnical Commission*

IETF - *Internet Engineering Task Force*

IPv4 - *Internet Protocol*

IPv6 - *Internet Protocol*

ISO - Organização Internacional para Padronização

ITI - Instituto Nacional de Tecnologia da Informação

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

Mac - *Macintosh*

NBR - Associação Brasileira de Normas Técnicas (ABNT)

PDF - *Portable Document Format*

RC - *Ron's Code ou Rivest Cipher*

RSA - *Rivest, Shamir and Adleman*

SHA - *secure hash algorithm*

WWW - *World Wide Web*

URI - *Uniform Resource Identifier*

XML - *Extensible Markup Language*

SOAP - *Simple Object Access Protocol*

RESUMO

Tomando-se a Internet como uma realidade e compreendendo-se as facilidades que ela traz a todos que a utilizam como instrumento de trabalho e negocio, viu-se a necessidade de criar soluções que protegessem esse ambiente e proporcionasse uma maior segurança nesse meio. Uma dessas soluções é a assinatura digital, que tem por função dar garantias da integridade e autenticidade de um documento. Composta por um conjunto de operações *criptográficas* aplicadas a um determinado arquivo, tendo como resultado o que se convencionou chamar de assinatura digital.

A massificação do uso da *internet* e a constante preocupação com a segurança das informações são os fatores motivacionais para o desenvolvimento deste trabalho.

Neste contexto, o projeto propõe o estudo e a implementação de um *plugin* especifico para navegadores o qual trará mais segurança e confiabilidade no momento da assinatura de um documento digital.

Palavras Chave: Assinatura Digital; *Internet*; Segurança da Informação; *Plugin*; Navegadores; Documento; Servidor.

ABSTRACT

Taking the Internet as a reality and by understanding the features it brings to all who use it as a working tool and business, we saw the need to create solutions that protect that environment and would provide greater security in the interim. One such solution is the digital signature, which is to provide assurance of the integrity and authenticity of a document. Consisting of a set of cryptographic operations applied to a particular file, resulting in the so-called digital signature.

The massification of Internet use and the constant concern for information security are the motivating factors for developing this work.

In this context, the project proposes the study and implementation of a specific plugin for browsers which will bring more security and reliability at the time of signing a digital document.

Keywords: *Digital Signature; the Internet; Information security; Plugin; browsers; Document; Server.*

SUMÁRIO

INTRODUÇÃO

Incontestavelmente a *internet* é o maior acontecimento em termos de tecnologia de todos os tempos. A qual possibilita uma maior rapidez e eficiência na produção, manuseio e transmissão de dados ou informações. Permitindo que milhões de pessoas se reúnam em torno de idéias em lugares virtuais, dessa forma, estabelece-se um novo protocolo de comunicação entre as pessoas, tanto físicas como jurídicas. Com isso surgem várias oportunidades de negócios na rede, tendo a informação como um produto de muita importância.

A manipulação indevida da informação pode ocasionar prejuízos, por isso requer alguns cuidados, especialmente em relação ao meio de divulgação e armazenamento utilizado. Podendo ocasionar diversos transtornos, pois a informação, na maioria das vezes, possui um valor seja emocional, financeiro ou qualquer outro valor agregado. Como a quantidade de informação que trafega na rede é grande, também é grande o número de pessoas tentando obter estas informações para benefício próprio.

Com as tecnologias atuais, tentativas de falsificação são cada vez mais freqüentes, o que acaba por diminuir a confiabilidade das informações transmitidas pela rede. Neste contexto, com a insegurança no momento da assinatura é necessário um cuidado cada vez maior. Juntamente com isso, novos mecanismos são desenvolvidos, visando o maior aperfeiçoamento, rapidez, confiabilidade, segurança e modernização do meio utilizado. São eles os documentos eletrônicos, a assinatura digital e as autoridades certificadoras.

OBJETIVOS GERAIS E ESPECIFICOS

O presente trabalho tem como objetivo, o desenvolvimento de um *plugin* para assinatura digital, a qual fará a comunicação com o *software* de assinatura 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). Onde o cliente selecionara o arquivo e todo o processo de assinatura será feito em *background.* Provendo um grau satisfatório na segurança das informações do Assinante.

Como objetivos específicos destacam-se:

- Estudo do Assinador Digital ICP - Brasil, implementação de referência em Java, desenvolvido em parceria entre LSI-TEC e o COMPSI;
- Estudo dos conceitos de *Web Services*;
- Estudo da tecnologia Apache *Tomcat* e suas características;
- Estudo do *framework Apache Axis*.
- Estudo da linguagem de Programação *JavaScript*; e
- Propor e desenvolver uma aplicação *Web* que realize todo o processo de assinatura de um documento seguindo os padrões do Assinador Digital ICP - Brasil em modo *background.*

ORGANIZAÇÃO DA MONOGRAFIA

O primeiro capítulo apresenta a metodologia sobre Segurança da Informação, *criptografia*, tipos de *criptografia* e maneiras se *criptografarem* uma mensagem. Apresentando a assinatura digital, o processo de assinatura de um documento.

O segundo capítulo apresenta os conceitos envolvidos na ICP – Brasil, referente sua validade no âmbito jurídico brasileiro, apresentando sua Infraestrutura de modo ao entendimento de sua hierarquia e funções, certificados digitais, assinatura digital, autoridades certificadoras (AC) e lista de certificados revogados.

O terceiro capítulo apresenta a tecnologia utilizada para o alcance do objetivo principal, o ‘Assinador Digital ICP – Brasil’, desenvolvido em parceria pelo LSI-TEC e o COMPSI, apresentando seus módulos e os processos na geração da assinatura digital, seguindo as normas da ICP - Brasil.

O quarto capítulo apresenta os requisitos funcionais do projeto, o fluxo de solução proposta para concretizar o projeto, as alterações realizadas no projeto

Inicial, as tecnologias utilizadas, e uma breve explicação de Serviço *Web*.

O quinto Capitulo descreve os Testes e Resultados Obtidos no decorrer do desenvolvimento do projeto, suas limitações e Desafios.

Por fim foi relatado as conclusões a respeito dos resultados obtidos, bem como as propostas de trabalhos futuros.

CAPITULO 1 - SEGURANÇA DA INFORMAÇÃO

O uso de sistemas informatizados para a realização das mais diversas atividades vem crescendo gradativamente nos últimos tempos, e, a integração destes sistemas e de suas bases de dados por meio de redes é um fato determinante da sociedade da informação. Contudo, este universo de conteúdos e continentes digitais está sujeito a várias formas de ameaças, físicas ou virtuais, que comprometem seriamente a segurança das pessoas e das informações a elas atinentes, bem como das transações que envolvem o complexo usuário, sistema e informação (MARCIANO, 2006).

> Quando se fala em segurança da informação, é necessário analisar todas as variáveis que podem influenciar a segurança. É necessário avaliar aspectos físicos, lógicos, humanos e suas relações. O aspecto mais importante em relação à segurança da informação, é que toda e qualquer ação deve ser tomada em função do negócio, deve agregar valor ao negócio de alguma forma, caso contrário, a segurança da informação é vista pela organização como um desperdício de recursos (CAMPOS, 2007; apud CARVALHO, 2011, P. 9)

A tecnologia da informação é capaz de apresentar parte da solução a este problema, não sendo, contudo, capaz de resolvê-lo integralmente, e até mesmo contribuindo, em alguns casos, para agravá-lo. Nos ambientes organizacionais, a prática voltada à preservação da segurança é orientada pelas chamadas políticas de segurança da informação, que devem abranger de forma adequada as mais variadas áreas do contexto organizacional, perpassando os recursos computacionais e de infra-estrutura e logística, além dos recursos humanos. (MARCIANO, 2006).

Portanto podemos dizer que não existe segurança absoluta, torna-se necessário agirmos no sentido de descobrir quais são os pontos vulneráveis e a partir daí avaliar os riscos e impactos, e rapidamente providenciar para que a segurança da informação seja eficaz.

1.1 Segurança da informação e seus Princípios

Segundo Albuquerque (2002, apud, LAUREANO; MORAES, 2005) e Krause (1999, apud, LAUREANO; MORAES, 2005) há três princípios básicos para garantir a segurança da informação:

- **Confidencialidade -** A confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso (NBR ISO/IEC 27002:2005). Caso a informação seja acessada por uma pessoa não autorizada, intencionalmente ou não, ocorre a quebra da confidencialidade. A quebra desse sigilo pode acarretar danos inestimáveis para a empresa ou até mesmo para uma pessoa física. Um exemplo simples seria o furto do número e da senha do cartão de crédito, ou até mesmo, dados da conta bancária de uma pessoa.

- **Integridade -** A integridade é a garantia da exatidão e completeza da informação e dos métodos de processamento (NBR ISO/IEC 27002:2005). “Garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente”. (DANTAS, 2011, p11). Quando a informação é alterada, falsificada ou furtada, ocorre à quebra da integridade. Sendo a integridade, garantida quando se mantém a informação no seu formato original.

- **Disponibilidade -** A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (NBR ISO/IEC 27002:2005). Quando a informação está indisponível para o acesso, ou seja, quando os servidores estão inoperantes por conta de ataques e invasões, considera-se um incidente de segurança da informação por quebra de disponibilidade. Mesmo as interrupções involuntárias do sistema, ou seja, não intencionais, configuram quebra de disponibilidade.

Ao se falar em segurança da informação, deve-se levar em consideração estes três princípios básicos, pois toda ação que venha a comprometer qualquer

uma desses princípios, seja confidencialidade, integridade ou disponibilidade, estará atentando contra a sua segurança

Outros autores (Dias, 2000; Wadlow, 2000; Shirey, 2000; Krause e Tipton, 1999; Albuquerque e Ribeiro, 2002; Sêmola, 2003; Sandhu e Samarati, 1994, apud LAUREANO, 2005) defendem o ponto de vista que para uma informação ser considerada segura, o sistema que o administra ainda deve respeitar:

- **Autenticidade** – Garante que a informação ou o usuário da mesma é autêntico; Atesta com exatidão, a origem do dado ou informação;
- **Não repúdio** – Não é possível negar (no sentido de dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação; Não é possível negar o envio ou recepção de uma informação ou dado;
- **Legalidade** – Garante a legalidade (jurídica) da informação; Aderência de um sistema à legislação; Característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.
- **Privacidade** – Foge do aspecto de confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve ser vista / lida / alterada somente pelo seu dono. Garante ainda, que a informação não será disponibilizada para outras pessoas (neste é caso é atribuído o caráter de confidencialidade a informação); É a capacidade de um usuário realizar ações em um sistema sem que seja identificado.
- **Auditoria** – Rastreabilidade dos diversos passos que um negócio ou processo realizou ou que uma informação foi submetida, identificando os participantes, os locais e horários de cada etapa. Auditoria em *software* significa uma parte da aplicação, ou conjunto de funções do sistema, que viabiliza uma auditoria; Consiste no exame do histórico dos eventos dentro de um sistema para determinar quando e onde ocorreu uma violação de segurança.

“Os benefícios evidentes são reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas

que possam comprometer estes princípios básicos". (ROCHA, 2008, p. 26).

Mesmo com toda essa política de segurança e a Norma BS 7799, considerada o mais completo padrão para o gerenciamento da Segurança da Informação. São necessários outros meios para garantirem a veracidade e autenticidade de uma informação. Dentro da área de segurança da informação possuímos alguns serviços, dentre eles a *criptografia*.

1.2 Criptografia

"Criptografia é caracterizada como a ciência (ou arte) de escrever em códigos ou em cifras, ou seja, é um conjunto de métodos que permite tornar incompreensível uma informação, de forma a permitir que apenas as pessoas autorizadas consigam decifrá-la e compreendê-la". (WEBER, 1995, p. 1).

Segundo (TERADA, 2008, p. 18) Algoritmos *criptográficos* basicamente objetivam "esconder" informações sigilosas de qualquer pessoa desautorizada a Lê-las, isto é, de qualquer pessoa que não conheça a chamada chave secreta de *criptografia*.

> Para (SIMON, 1999, apud MORENO, PEREIRA, CHIARAMONTE, 2005, p. 21) A criptografia pode ser entendida como um conjunto de métodos e técnicas para cifrar ou codificar informações legíveis por meio de um algoritmo, convertendo um texto original em um texto ilegível, sendo possível mediante o processo inverso recuperar as informações originais.

Atualmente, a *criptografia* é considerada uma ramificação da criptologia, que, por sua vez, dado o grau de sofisticação e embasamento teórico que envolvem o seu estudo, é hoje considerada uma ciência, no campo das Ciências Exatas. (MARCACINI, 2010).

Podendo *criptografar* informações basicamente por meio de códigos ou de cifras. Os códigos protegem as informações trocando partes destas por códigos predefinidos

1.2.1 Maneiras de Criptografar Mensagens

> Para (TRINTA; MACÊDO, 1998) Há duas maneiras básicas de se criptografar mensagens: através de códigos ou através de cifras. O primeiro procura esconder o conteúdo da mensagem através de códigos predefinidos entre as partes envolvidas na troca de mensagens. Imagine o exemplo onde em uma guerra, um batalhão tem duas opções de ação contra o inimigo: atacar pelo lado direito do inimigo ou não atacar. A decisão depende da avaliação de um general posicionado em um local distante da posição de ataque deste batalhão. É acertado que se for enviado uma mensagem com a palavra "calhau", o exército deverá atacar pela direita; se for enviada uma mensagem com a palavra "araçagy", não deve haver ataque. Com isso, mesmo que a mensagem caia em mãos inimigas, nada terá significado coerente. O problema deste tipo de solução é que com o uso constante dos códigos, eles são facilmente decifrados. Outro problema é que só é possível o envio de mensagens predefinidas. Por exemplo: não há como o general mandar seu exército atacar pela esquerda.

Segundo (MORENO; PEREIRA; CHIARAMONTE, 2005) As cifras são técnicas nas quais a informação é cifrada por meio da transposição e/ou substituição das letras da mensagem original. Assim, as pessoas autorizadas podem ter acesso ás informações originais conhecendo o processo de cifragem.

Logo abaixo observa-se na Figura 1, um pequeno esquema do processo de cifragem e decifragem de um documento, onde é aplicado no arquivo o algoritmo de Cifragem, gerando um texto cifrado, em seguida sendo aplicado um algoritmo de decifragem, gerando assim o documento normal.

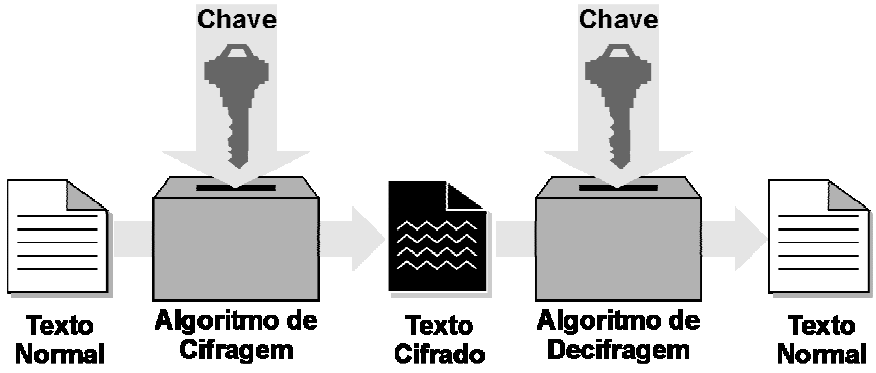


Figura 1. Cifragem e decifragem de uma mensagem (TRINTA; MACÊDO, 1998)

1.2.2 Tipos de Criptografias

Segundo (MARCACINI, 2010) “Existem dois métodos diferentes de se *criptografar* uma mensagem: por *criptografia* simétrica ou por *criptografia* assimétrica”.

Criptografia Simétrica:

Na *criptografia* simétrica a mesma chave é utilizada tanto pelo emissor quanto por quem recebe a informação. Ou seja, a mesma chave é utilizada para codificação e para a decodificação dos dados.

Entre os algoritmos que usam essa chave, estão:

- ***DES (Data Encryption Standard):*** Faz uso de chaves de 56 bits, que corresponde à aproximadamente 72 quatrilhões de combinações. Mesmo sendo um número absurdamente alto, em 1997, conseguiram quebrar esse algoritmo através do método de 'tentativa e erro', em um desafio na *internet.*
- ***RC (Ron's Code ou Rivest Cipher):*** É um algoritmo muito utilizado em *e-mails* e usa chaves de 8 a 1024 bits, além de possuir várias versões que se diferem uma das outras pelo tamanho das chaves.
- **AES *(Advanced Encryption Standard*)**: Hoje em dia é um dos melhores e mais populares algoritmo de *criptografia* existente. Você pode definir o tamanho da chave como sendo de 128bits, 192bits ou 256bits.
- ***IDEA (International Data Encryption Algorithm):*** É um algoritmo que usa chaves de 128 bits, parecido com o *DES.* Seu ponto forte é a fácil implementação de *software*.

Não sendo totalmente seguras quando se trata de informações muito valiosas, principalmente pelo fato de que o emissor e o receptor têm que conhecer a mesma chave. Assim, a transmissão pode não ser segura e o conteúdo chegar a terceiros.

Criptografia Assimétrica:

A *criptografia* assimétrica utiliza duas chaves diferentes, porém matematicamente relacionadas, para *criptografar* e *descriptografar* dados. Essas

chaves são conhecidas como chaves privadas e chaves públicas. Em conjunto, essas chaves são conhecidas como par de chaves.

Sendo resumidas da seguinte forma, Alguém deve criar uma chave de codificação e enviá-la a quem for lhe mandar informações. Essa é a chave pública. Outra chave deve ser criada para a decodificação. Esta, a chave privada, levando-se em consideração que a chave privada é secreta.

Entre os algoritmos utilizados, estão:

- ***RSA (Rivest, Shamir and Adleman):*** Criado por três professores do MIT, é um dos algoritmos mais usados e bem-sucedidos, utiliza dois números primos (aqueles que só podem ser divididos por 1 e por eles mesmos) são multiplicados para a obtenção de um terceiro valor. Para isso, é preciso fazer fatoração, que é descobrir os dois primeiros números a partir do terceiro, que é um cálculo trabalhoso. Assim, se números grandes forem utilizados, será praticamente impossível descobrir o código. A chave privada do *RSA* são os números que são multiplicados e a chave pública é o valor que será obtido. Utilizada em *sites* de compra e em mensagens de *e-mail.*

- ***ElGamal:*** Criado pelo estudioso de *criptografia egípcio Taher Elgamal* em 1984 Utiliza-se o problema do 'logaritmo discreto', que é um problema matemático que o torna mais seguro. É bastante utilizado em assinaturas digitais.

A Figura 2 apresenta o processo de *criptografia* por chave publica (assimétrico). Onde é gerado um par de chaves, e enviado a (publica) chave-pública para a pessoa desejada. Esta pessoa cifra a mensagem com a chave-pública que recebeu, a qual, somente quem enviou será capaz de decifrá-la, utilizando sua chave-privada.

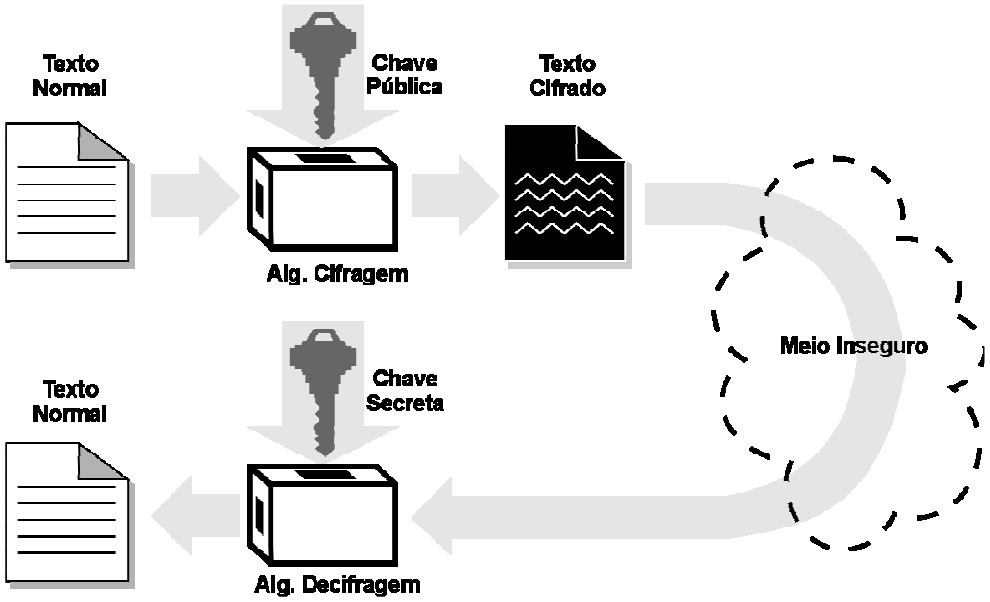


Figura 2. Processo de criptografia por chave pública (TRINTA; MACÊDO, 1998).

Portanto, os algoritmos que são utilizados para a *criptografia* simétrica são muito mais rápida, no entanto são mais simples do que os algoritmos usados na *criptografia* assimétrica.

Sendo uma das principais desvantagens da *criptografia* simétrica o uso da mesma chave tanto para *criptografar* como para *descriptografar* os dados. Por isso, todas as partes que enviam e recebem os dados devem conhecer ou ter acesso à chave de *criptografia.* Esse requisito cria um problema de gerenciamento de segurança e problemas de gerenciamento de chave que uma organização deve considerar em seu ambiente.

A *criptografia* simétrica fornece autorização para dados criptografados. Por exemplo, ao usar a *criptografia* simétrica, uma organização pode estar razoavelmente certa de que apenas as pessoas autorizadas a acessar a chave de *criptografia* compartilhada podem *descriptografar* o texto codificado. No entanto, a *criptografia* simétrica não fornece não-repúdio. Por exemplo, em um cenário em que vários grupos têm acesso à chave de *criptografia* compartilhada, a *criptografia* simétrica não pode confirmar o grupo específico que envia os dados.

> **Como provar que um algoritmo criptográfico é seguro.? Caso AES.**
>
> Até hoje (2000) não se conhece um método matemático para provar que um algoritmo criptográfico é seguro. A maneira mais próxima deste ideal que se conhece é publicá-lo (por exemplo, nas conferencias CRYPTO e EUROCRYPT) e te-lo analisado pelos pesquisadores especializados que conheçam os métodos mais sofisticados para atacá-lo. Se o algoritimo [sic] passa por tal escrutínio, a industria aceita-o como seguro em relação ao estado-da-arte.(TERADA, 2008, p 21)

Sendo a assinatura digital o grande beneficio da *criptografia* com chave pública, que diferentemente dos algoritmos de *criptografia* simétrica, possuem não só uma única chave, e sim duas chaves, uma privada e outra pública que são usadas para *cifrar* e *decifrar* respectivamente o documento. Sendo a assinatura digital o grande enfoque do trabalho, onde permite garantir a autenticidade de quem envia a mensagem, associada a integridade do seu conteúdo e o não repudio ou irretratabilidade, onde o emissor não poderá, por forças tecnológicas e legais, negar que seja o responsável por seu conteúdo, sendo a Infraestrutura de Chaves Públicas Brasileira (ICP - Brasil) uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão.

Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o Instituto Nacional de Tecnologia da Informação (ITI) uma autarquia federal vinculada à Casa Civil da Presidência da República, cujo objetivo é manter a Infraestrutura de Chaves Públicas Brasileiras – ICP - Brasil, além de desempenhar o papel de Autoridade Certificadora Raiz (AC - Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

> "Art. 1º Fica instituída a Infra-Estrutura 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." (Medida Provisória Nº2.200-2 de 24 de agosto de 2001)

1.3 Assinatura Digital

Para (ALVES, 2013) 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, sendo utilizado algumas técnicas de *criptografia*.

Toda essa precaução se faz necessária no dia a dia, devido a grande quantidade de crimes digitais que acorrem no mundo diariamente. Estima-se que dois terços dos internautas do mundo já foram vítimas de algum crime digital segundo um estudo divulgado em 2010 pela *Symantec*. Durante a pesquisa foram entrevistados 7 mil adultos de 14 países. Segundo o estudo, chamado de "*Norton Cybercrime Report: The Human Impact*", sendo a china, Índia e Brasil os países que possuem mais vítimas de ataques. Dados preocupantes para a população Brasileira.

Com tantos crimes e perigos no mundo virtual a assinatura digital é um meio seguro de comprovar a procedência de um documento. Com a utilização de uma espécie de "chave", esse sistema se torna um alvo difícil para fraudes pela sua complexidade.

Outro trunfo da assinatura digital é que, com o crescente número de pessoas e empresas usando esse artifício, foi necessário organizar e padronizar essas operações. A ICP - Brasil faz isso por meio da certificação digital e das assinaturas das AC (Autoridade Certificadora). Com os certificados digitais devidamente assinados e com os devidos cuidados, os riscos da assinatura digital não funcionar é mínima.

1.3.1 Assinando Digitalmente um Documento

Segundo (VIEIRA, 2012) "Existem diversas maneiras de assinar digitalmente um documento, mas a forma mais usual e eficaz envolve processos criptográficos utilizando algoritmos de funções unidirecionais ou *hash* criptográficos".

As funções *hash*, também denominada *Message Digest, One-Way Hash Function*, Função de Espalhamento Unidirecional é um mecanismo fundamental para as assinaturas digitais. Pois ao usar apenas algoritmos de chave pública e privada nas Assinaturas Digitais e ao assinar documentos grandes gastaria muito tempo devido á lentidão dos algoritmos. Ao invés disso, é empregada uma função *Hashing*,

obtida por meio de algoritmos de *criptografia* (SHA-256, SHA-512, os mais utilizados no momento) que gera um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar. De um contexto geral, seria uma transformação de uma grande quantidade de informações em uma pequena quantidade de informações, que nada mais é do que a transformação das informações de um documento em uma seqüência de bits. Assim a função *Hashing* oferece agilidade nas assinaturas digitais (NORÕES, 2008 apud VIEIRA, 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 descriptografa 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 modificada, caso contrário, alguma violação ocorreu na mensagem (ICP - Brasil, 2012 apud ALVES, 2012).

Resumindo, o processo de assinatura segue os seguintes passos: é gerado um *hash* do documento que deseja ser assinado, este *hash* é cifrado com a chave privada do assinante, o resultado obtido pode ser chamado de assinatura, esta assinatura é vinculada de alguma forma ao documento original. Para atender a validade temporal é utilizado a assinatura de um terceiro confiável responsável em fornecer o tempo de forma segura, estes são chamados autoridades de carimbo de tempo (ACT) (TOGNOLI, 2012).

Na figura 3 é apresentada a troca de uma mensagem assinada entre duas entidades, também sendo demonstrando a forma de verificação da assinatura.

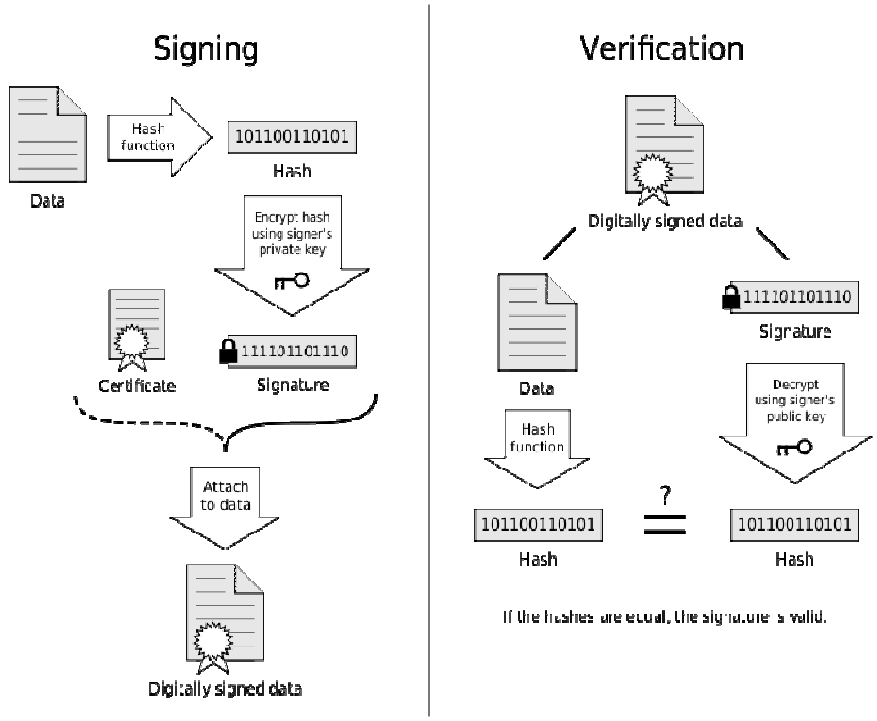


Figura 3. Esquematização das etapas de Geração e Validação da Assinatura Digital (Universidade Federal do Rio de Janeiro - Engenharia de Controle e Automação, 2010).

1.4 Carimbo de Tempo

Carimbos de tempo são documentos eletrônicos assinados por uma terceira parte confiável, denonimada Autoridade de Carimbo do Tempo (ACT), onde consta tanto o resumo criptográfico da informação datada, quanto a data em que o carimbo foi emitido. São duas as operações relacionadas a esses carimbos, a sua solicitação e validação.

Um carimbo do tempo é valido se:

- A assinatura da ACT for valida;
- O resumo criptográfico presente no carimbo for uma função de resumo criptográfico segura.

Tais condições visam comprovar, respectivamente, a autenticidade do carimbo e a integridade da informação datada (SILVA, Nelson; RAMOS, Thiago Acórdi; CUSTÓDIO, Ricardo Felipe).

Segundo (ITI, 2012) carimbo de tempo é um documento eletrônico emitido

por uma parte confiável, que serve como evidência de que uma informação digital existia numa determinada data e hora no passado. Destina-se a associar a um determinado *hash* de um documento assinado eletronicamente ou não, uma determinada hora e data de existência. Ressalta-se que o carimbo de tempo oferece a informação de data e hora de registro deste documento quando este chegou à entidade emissora, e não a data de criação deste documento.

Analisando todo esse contexto, há principio utilizarei a Assinatura digital para assinar documentos acadêmicos por meio de navegadores *web* (*internet*), tendo como objetivo fixar esse mecanismo dentro de navegadores, por meio de *plugin*.

1.5 Considerações Finais do Capitulo

No quesito tecnologia as políticas de segurança sempre serão bem-vindas para que tudo ocorra como tem que ser no universo dos negócios e na *internet*. A assinatura digital é uma opção interessante e vai se tornando cada vez mais indispensável para quem quer sobreviver bem em negócios online (*e-commerce*), transmitindo segurança a um documento eletrônico, garantindo sua integridade, autenticidade e não repúdio.

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

CAPITULO 2 - INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA (ICP - BRASIL)

A Infraestrutura de Chaves Pública Brasileira (ICP - Brasil) é um conjunto de técnicas, práticas e procedimentos que foram traçadas pelo seu Comitê Gestor com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública. Sendo uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão.

Segundo a MEDIDA PROVISÓRIA No 2.200-2, DE 24 DE AGOSTO DE 2001 Art. 1º Fica instituída a Infra-Estrutura de Chaves Pública 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.

Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI – Instituto Nacional de Tecnologia da Informação, autarquia federal vinculada à casa Civil da Presidência da Republica, além de desempenhar o papel de Autoridade Certificadora Raiz (AC - Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

> Segundo (BARRA, 2006) A ICP-Brasil visa proporcionar uma resposta para a questão que o aparecimento desse novo meio de comunicação impunha: como acreditar em algo na Internet? Como enviar pela rede um documento assinado, e que obtenha o mesmo valor juridico de um documento assinado de próprio punho? A ICP-Brasil foi instituida pelo Estado brasileiro como um mecanismo que possibilita a chamada "Assinatura digital". com a validade reconhecida por esse Estado e por intermédio dele.

2.1 Autoridade Certificadora (AC) e Autoridades de Registros(AR)

AC – Raiz

A Autoridade Certificadora Raiz da ICP - Brasil (AC - Raiz) é a primeira autoridade da cadeia de certificação. Tem como função básica a execução das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê

Gestor da ICP - Brasil, atuando: na emissão, expedição, distribuição, revogação e gerenciamento de certificados de autoridades certificadoras de nível imediatamente inferior ao seu, chamadas Autoridades Certificadoras Principais.

AC - Autoridade Certificadora

Uma Autoridade Certificadora (AC) é uma entidade, pública ou privada, subordinada à hierarquia da ICP - Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (público-privada).

Cabe também à AC emitir listas de certificados revogados (LCR) e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação (DPC). Além de estabelecer e fazer cumprir, pelas Autoridades Registradoras (ARs) a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação realizada.

AR - Autoridade de Registro

As Autoridades de Registro (ARs) são as responsáveis pelo processo final na cadeia de Certificação Digital, responsáveis por atender os interessados em adquirir certificados, coletar os documentos para encaminhá-los às Autoridades Certificadoras (ACs), responsáveis pela emissão. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.

A Diretoria de Auditoria, Fiscalização e Normalização do ITI – Instituto Nacional de Tecnologia da Informação reuniu as exigências direcionadas às Autoridades Registradoras (AR), segundo as resoluções da ICP - Brasil. Trata-se de um guia para auxiliar no entendimento das exigências para o funcionamento das ARs. Maiores informações são encontradas na Instrução Normativa nº 07/2006, anexo ao documento DOC-ICP-03.

ACT - Autoridade Certificadora do Tempo

Uma Autoridade Certificadora do Tempo (ACT) é uma entidade na qual os usuários de serviços de Carimbo do Tempo confiam para emitir Carimbos do Tempo. A ACT tem a responsabilidade geral pelo fornecimento do Carimbo do Tempo, conjunto de atributos fornecidos pela parte confiável do tempo que, associado a uma assinatura digital, confere provar a sua existência em determinado período.

Na prática, um documento é produzido e seu conteúdo é criptografado. Em seguida, ele recebe os atributos ano, mês, dia, hora, minuto e segundo, atestado na forma da assinatura realizada com certificado digital servindo assim para comprovar sua autenticidade. A ACT atesta não apenas a questão temporal de uma transação, mas também seu conteúdo.

2.2 Estrutura 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.

A AC - Raiz é o Instituto Nacional de Tecnologia da Informação – ITI, autarquia federal vinculada à Casa Civil da Presidência da República que também está encarregada de emitir a lista de certificados revogados (LCR) e de fiscalizar e auditar as Autoridades Certificadoras (ACs), Autoridades de Registro (ARs) e demais prestadores de serviço habilitados na ICP - Brasil. Além disso, verifica se as ACs estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP - Brasil.

Veja a estrutura resumida da ICP - Brasil apenas com as Autoridades Certificadoras de 1º Nível e de 2º Nível, ilustrada na Figura 4.

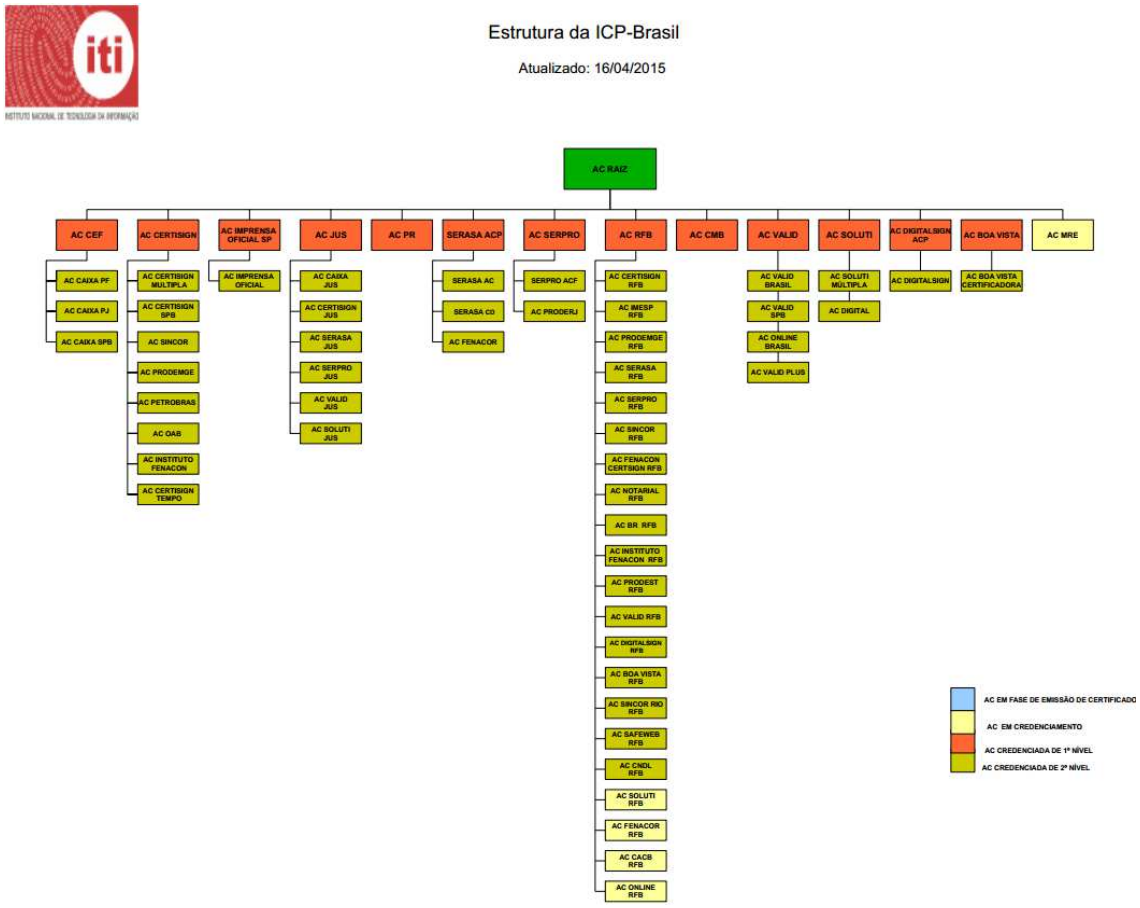


Figura 4. Estrutura da ICP - Brasil (ITI, 2015).

2.3 Certificados Digitais ICP – Brasil

Os Certificados Digitais é uma assinatura com validade jurídica que garante proteção às transações eletrônicas e outros serviços via *internet*, permitindo que pessoas e empresas se identifiquem e assinem digitalmente de qualquer lugar do mundo com mais segurança e agilidade.

Segundo (ALVES, 2013) 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 do arquivo assinada. Diante deste panorama, necessita-se de uma terceira parte confiável, que garanta tais informações, o certificado digital surge com esse propósito.

Na prática, o certificado digital funciona como uma identidade virtual que

permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a *web*. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas pelo Comitê Gestor da ICP - Brasil associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas. Os certificados contêm os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora (ITI, 2015).

Logo abaixo a Figura 5, ilustra um certificado no momento de sua instalação.

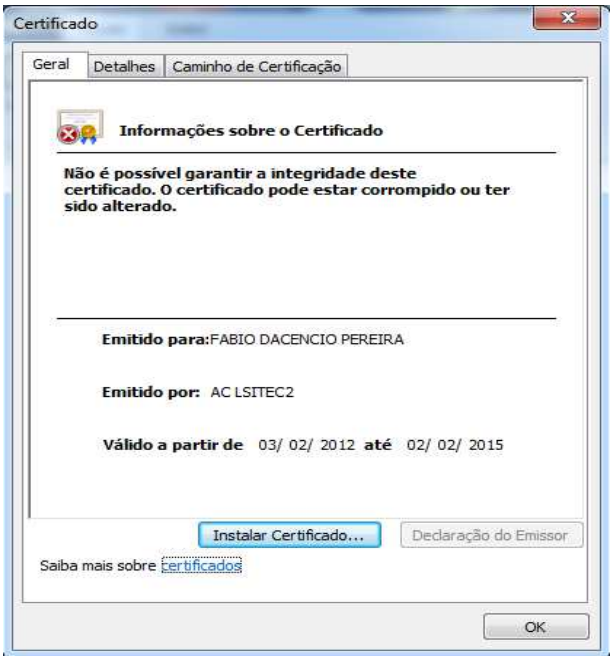


Figura 5. Certificado Digital. (Própria).

O certificado digital da ICP - Brasil, além de personificar o cidadão na rede mundial de computadores, garante, por força da legislação atual, validade jurídica aos atos praticados com o seu uso. Permitindo que aplicações como comércio eletrônico, assinatura de contratos, operações bancárias, iniciativas de governo eletrônico, entre outras, sejam realizadas. São transações feitas de forma virtual, ou seja, sem a presença física do interessado, mas que demanda identificação clara da pessoa que a está realizando pela *internet*.

A Figura 6 apresenta alguns certificados instalados no computador, para a realização de alguns testes.

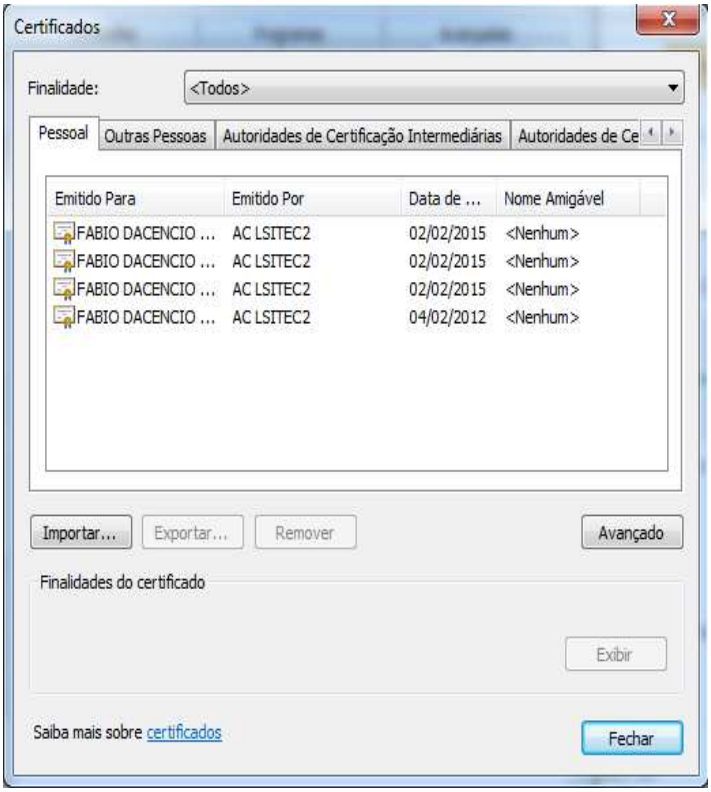


Figura 6. Certificado instalado. (Própria).

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).

2.3.1 Tipos de certificados digitais

Certificado do tipo A1

[1] Validade de 12 meses.

[2] Geração do par de chaves realizada em estação de trabalho.

Certificados do tipo A3

a) Validade de 36 meses.

b) Geração do par de chaves em mídias criptográficas (*Token* ou *SmartCard*).

Certificados do tipo A3 para Micro e pequenas empresas

a) Validade de 18 meses.

b) Geração do par de chave em mídias criptográficas (*Token* ou *SmartCard*).

2.4 Documentos Principais

Para regulamentar a infra-estrutura e certificado digitais, a ICP – Brasil criou algumas resoluções, das quais, o ETI publicou uma versão organizada de forma a facilitar a leitura e compreensão daquele que as estuda. Apresentando apenas o conteúdo referente á determinada regra imposta por esta resolução.

Cada DOC-ICP corresponde a uma resolução vigente. Estando disponível no site: http://www.iti.gov.br/legislacao/143-icp-brasil/legislacao/790-doc-icp

2.5 Verificador de Conformidade

Para a verificação de conformidade com padrão de assinatura ICP - Brasil, o ITI criou um *software* verificador de certificado de assinatura digital.

O Presente serviço tem por objetivo aferir a conformidade de um arquivo assinado com certificado ICP – Brasil de acordo com as normas previstas no DOC ICP – 15.

1. Possui como função atestar a observância do padrão estabelecido no DOC ICP-15, de modo que as eventuais invalidades verificadas pelo *software* devem ser tratadas com o provedor do assinador digital e não significam que o documento seja inválido, mas, apenas, que não são seguidas as especificações do DOC em referência;

2. Não valida quaisquer conteúdos assinados, sendo de inteira responsabilidade do usuário a veracidade e a comprovação das informações perante terceiros;

3. É um *software* disponibilizado de forma gratuita;

4. Não armazena quaisquer informações;

5. O ITI não se responsabiliza por eventuais danos causados pelo seu uso em quaisquer de suas versões, bem como não se compromete a prestar suporte técnico;

6. Excepcionalmente, o sistema poderá estar indisponível sem prévio aviso;

Segundo o assessor técnico do ITI, Ruy Ramos, além de auxiliar na divulgação dos padrões de assinatura da ICP - Brasil, o verificador trará mais segurança para empresas que pretendem obter ou desenvolver assinadores de arquivos.

Vale ressaltar que o verificador atesta a conformidade apenas de arquivos previstos no DOC ICP-15, que traz uma visão geral sobre assinaturas digitais na ICP - Brasil e define os principais conceitos e lista os demais documentos que compõem as normas da ICP - Brasil sobre o assunto, de modo que as eventuais invalidades verificadas devem ser tratadas com o provedor do assinador digital. Isso não significa que o documento seja inválido, mas, apenas, que não são seguidas as especificações do DOC em referência.

Por isso antes de utilizar o verificador é importante saber se o documento a ser submetido está previsto no DOC de referência.

O uso do verificador é bem simples. Após ler e aceitar a política de uso do aplicativo, o usuário é direcionado para página onde deve selecionar a assinatura e o arquivo que deseja verificar. Após escolher os arquivos, basta clicar em gerar relatório (ITI, 2014).

O serviço pode ser acessado pelo seguinte site: https://verificador.iti.gov.br.

2.6 Considerações Finais do Capitulo

A instituição da Medida Provisória 2.200-2 de 24 de agosto de 2001 estabelece toda a infra-estrutura 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, de modo que possam substituir os documentos em papel pelos documentos eletrônicos.

Sendo a AC - Raiz a autoridade certificadora mais importante no âmbito da ICP - Brasil sendo responsável pela emissão dos certificados de todas as Autoridades Certificadoras.

Por fim, não satisfeito com a segurança atual que ha nos padrões ICP – Brasil o ITI disponibilizou um Verificador de conformidade, que reforçara ainda mais essa questão da segurança, para empresas e pessoas físicas. Um mecanismo a mais para aqueles que utilizam a assinatura digital.

CAPITULO 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, seguindo as normas e estruturas estabelecidas pela ICP - Brasil. Realizando vários tipos de verificações que podem ser feitas desde verificações de lista de certificados revogados, para certificados com lista que estão taxadas ou hospedados em algum outro servidor, verificações temporais, cadeia de certificados, verificar em um certificado digital sua respectiva assinatura. E por fim, verificar políticas de certificados.

Um certificado ICP - Brasil possui algumas validações na qual são implantadas após o documento já estar devidamente assinado, onde se destaca a validação da Assinatura que se torna indispensável na verificação da real autoria do documento, validação de tempo, aspectos de revogação, validações de algoritmos criptográficos dentre outras validações especificas para representar uma pessoa jurídica ou uma pessoa física.

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, 2013).

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, as figuras 7, 8 e 9 ilustram o fluxo básico da geração de um arquivo assinado. (Alves, 2013).

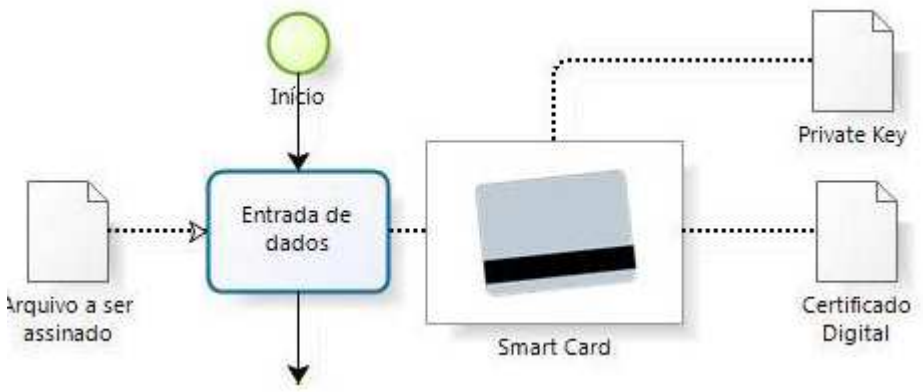


Figura 7. Fluxo da Geração de um Arquivo Assinado. (Alves, 2012).

A figura 7 retrata o momento em que é selecionado o arquivo a ser assinado, e também a inserção do *SmartCard* para uma posterior assinatura.

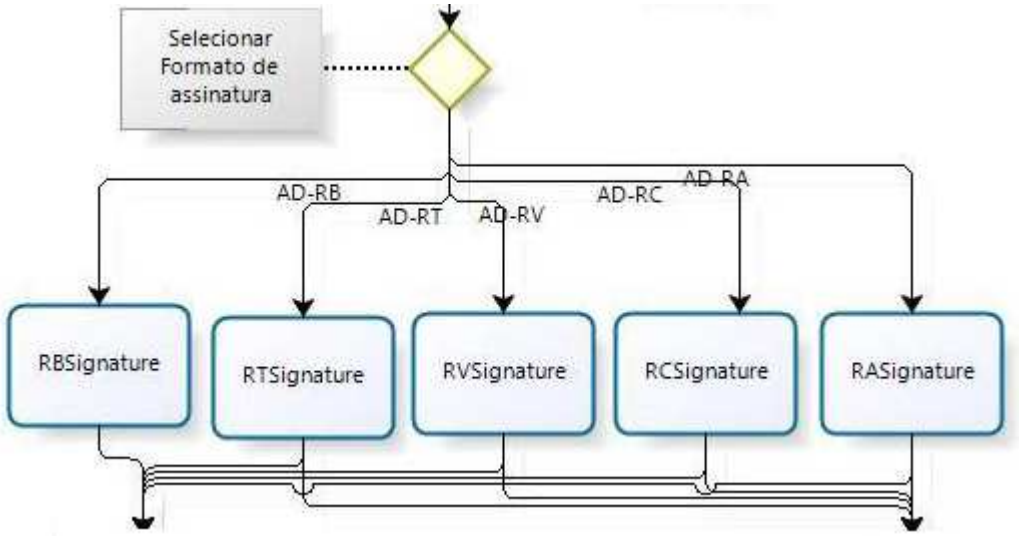


Figura 8. Fluxo da Geração de um Arquivo Assinado. (Alves, 2012).

Na seqüência, a figura 8 mostra o instante onde é selecionado o formato para a assinatura, sendo estes:

AD-RB - Assinatura digital com Referência Básica
AD-RT - Assinatura digital com Referência de Tempo
AD-RV - Assinatura digital com Referências para Validação
AD-RC - Assinatura digital com Referências Completas
AD-RA - Assinatura digital com Referências para Arquivamento

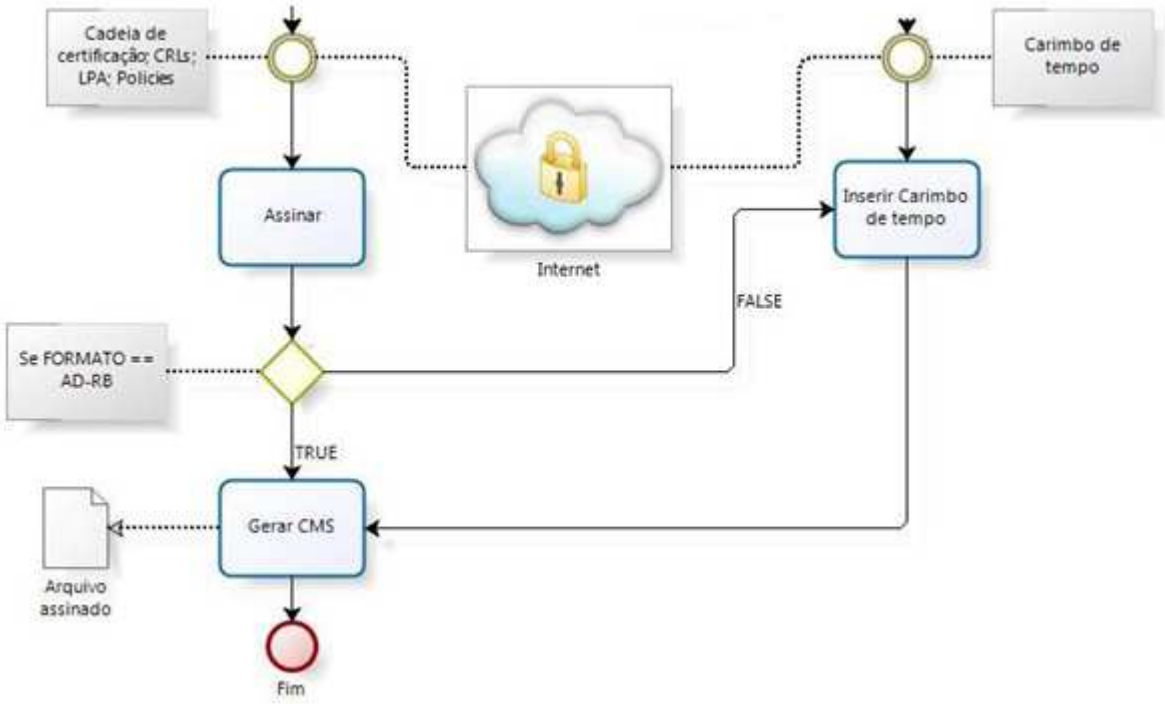


Figura 9. Fluxo da Geração de um Arquivo Assinado. (Alves, 2012).

E para concluir, na figura 9 demonstra o processo final da assinatura, onde a mesma mostra a utilização do carimbo de tempo e a respectiva geração do CMS, ou seja, a estrutura básica de um documento eletrônico assinado, que é gerado a partir dos dados de entrada.

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, 2013).

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. Sendo realizadas algumas modificações para que o carimbador de tempo pudesse estar em acordo com as normas estabelecidas pela ICP – Brasil. Sendo 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

Como a API Assinador Digital ICP - Brasil, desenvolvida pelo LSI-TEC e o COMPSI atende todos os requisitos e normas estabelecidas pela ICP – Brasil, é possível a utilização da mesma como auxilio para o desenvolvimento de um *plugin* de assinatura digital *Web* de documentos eletrônicos validos no âmbito jurídico brasileiro.

O próximo capítulo apresenta as ferramentas, e a forma com que foi desenvolvido o *plugin* de assinatura digital ICP - Brasil para navegadores *Web*.

CAPITULO 4 – PLUGIN DE ASSINATURA DIGITAL – WEB

A partir de um projeto desenvolvido por ALVES, 2012, onde o mesmo propõe-se a implementação de um *Web Service* para a assinatura digital, surgiu a oportunidade de melhorias no projeto original, implementando um *plugin* que realizara todo o processo de assinatura em modo *background*, do lado do cliente.

Onde o mesmo simplesmente selecionara o arquivo que se deseja assinar e todo o processo de assinatura, será realizado localmente, em segundo plano (*background*). Além dos estudos realizados a respeito de conceitos e ferramentas, foi utilizado como base para a realização do projeto proposto a API assinador digital ICP - Brasil, *software* 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).

Sendo que o cliente selecionara o arquivo para ser assinado e no momento da assinatura a aplicação ira verificar se o computador possui o app.jar (Assinador ICP - Brasil), caso contrario ele é redirecionado para o servidor Web para realizar o download do arquivo app.jar, esse arquivo é armazenado localmente em seu computador dando continuidade no processo de assinatura.

4.1 Requisitos Funcionais da Proposta

- Comunicação entre aplicação Web e o Assinador Digital ICP - Brasil
- Assinador ICP - Brasil Sendo Executado em Segundo Plano
- Verificação local do Arquivo
- Requisição ao Servidor Web
- Download do Arquivo no Servidor Web
- Log com Informações do Assinador.

4.2 Fluxo de Solução proposta

A Figura 10 representa o diagrama completo da aplicação *Web* de Assinatura Digital ICP – Brasil, destacando-se todas as etapas da aplicação, desde o momento em que é selecionado o arquivo a ser assinado até a criação do Arquivo Log, contendo todas as informações necessárias para a conclusão da Assinatura.

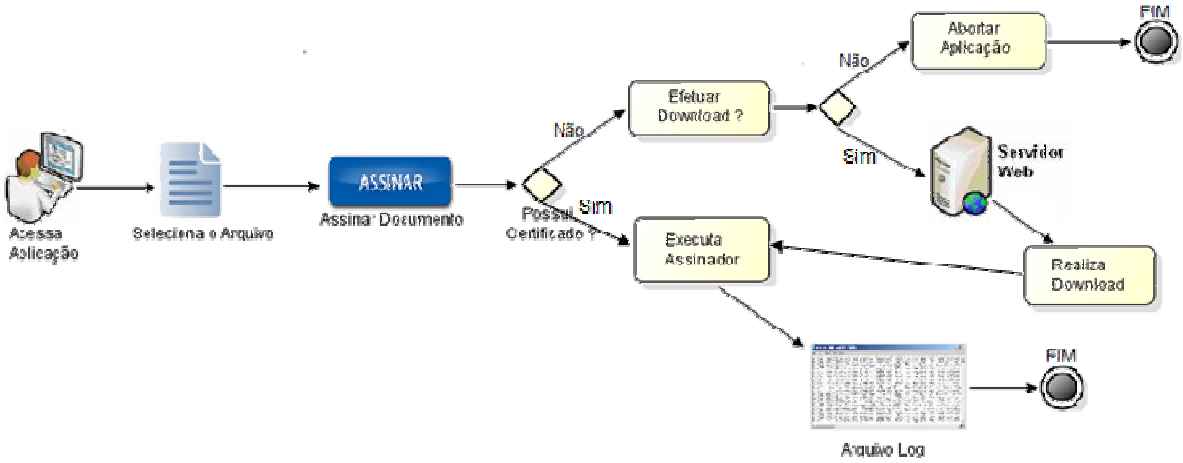


Figura10. Diagrama Aplicação Web de Assinatura Digital (Própria).

A Figura 11. Destaca-se o momento em que o Usuário acessa a aplicação, Seleciona o arquivo que se deseja assinar e pressiona o botão para assinar, onde será disparado todos os eventos para concretização do processo de assinatura.

Figura 11. Diagrama Selecionar Arquivo. (Própria).

Já a figura 12, representa a tela de testes de seleção do arquivo.

Passos:

1) Procurar Arquivo ;
2) Local onde o Endereço do Arquivo será carregado;
3) Realizar a Assinatura;

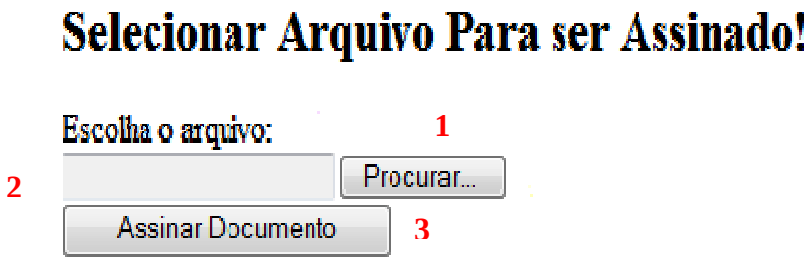


Figura 12. Selecionar Arquivo. (Própria).

Logo abaixo na Figura 13 é representado o momento em que ao clicar no botão Assinar, será disparado o evento em que a aplicação verificara se a maquina local possui o arquivo do Assinador, caso ela possua, esse arquivo será executado, caso contrario, o cliente terá a opção de realizar o *Download* ou não.

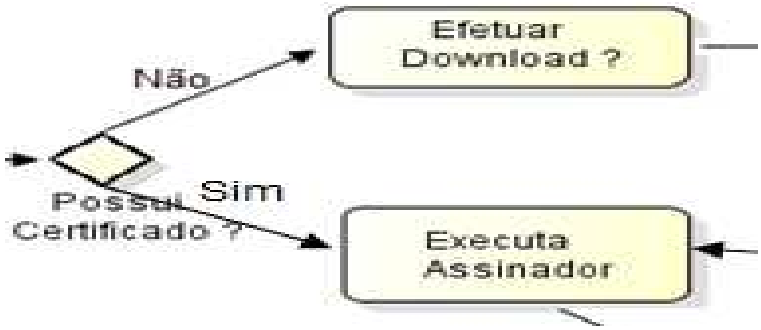


Figura 13. Diagrama Verifica se a maquina Local possui o Arquivo. (Própria).

Na figura 14 é destacado o código fonte da funcionalidade mencionada acima, onde a variável ‘comando’ ira receber o endereço do assinador juntamente

com o endereço do arquivo que se deseja assinar armazenado na variavel ‘pathArquivo.value’. Caso esse endereço ‘C:\\app’ não for encontrado o cliente será alertado que o Assinador não foi encontrado e se ele gostaria de estar realizando o Download desse arquivo.

```
var comando = "C:\\app\\dist\\app.jar " + pathArquivo.value;

//app.run(comando);
try{
    app.run(comando)
    }catch(e){

     var opcao = confirm("Assinador Não Encontrado. Gostaria de realizar o Download.?");
```

Figura 14. Execução do Assinador. (Própria).

A Figura 15 apresenta o momento em que o cliente não possui o assinador na sua maquina, e tem a possibilidade de efetuar o *download* desse assinador ou não. Caso não deseja realizar o *download*, a aplicação simplesmente é abortada. Caso queira realizar o *download*, será efetuada uma requisição ao servidor *Web*, solicitando o *Download* do Arquivo.

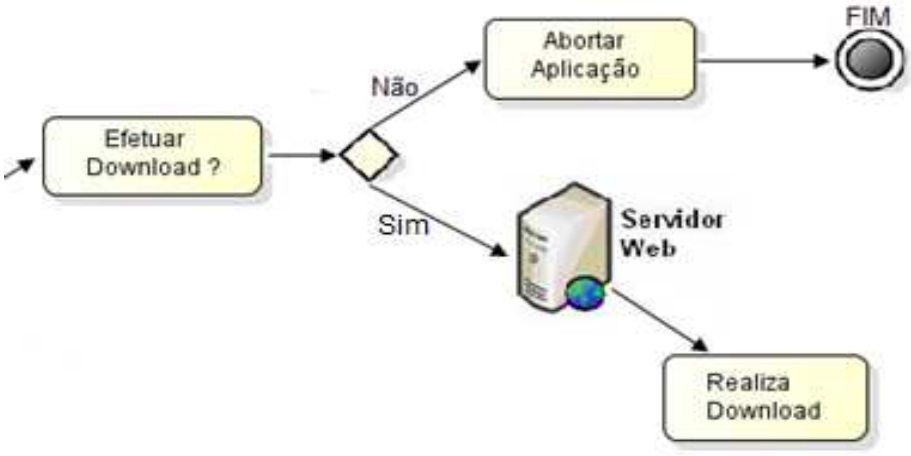


Figura 15. Diagrama Opção para realizar o Download

Na figura 16 é destacado o código fonte da requisição destacada acima. Onde ao clicar em ‘Ok’ para concretizar o *download*, será informado uma mensagem

para que o Usuário aguarde alguns Instantes pois o *Download* será realizado. Em seguida é executado o arquivo 'RequisicaoWEB.exe' que será responsável em realizar todo o processo de *download* e verificação do Arquivo.

Caso o cliente cancele a Operação, ele simplesmente recebera um alerta informando que a aplicação será abortada.

```
var opcao = confirm("Assinador Não Encontrado. Gostaria de realizar o Download.?");
if (opcao){
    alert("Aguarde Alguns Instantes. Arquivo sendo Baixado.!");
    var chamaBat = "C:\\Users\\Marquinho\\Desktop\\ArquivoEXEC\\RequisicaoWEB.exe";
app.run(chamaBat);

}
else
   alert("Aplicação abortada.!");
```

Figura 16. Código Fonte realizar Download ou abortar aplicação.

A figura 17 representa a requisição ao servidor e o respectivo *Download* do arquivo.

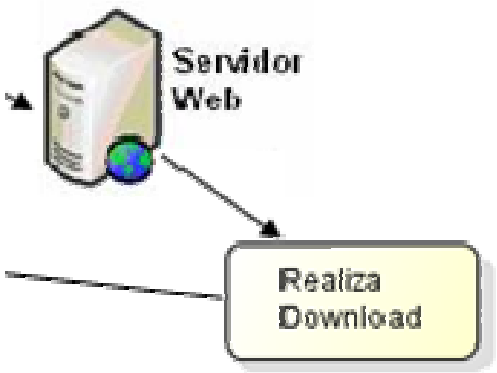


Figura 17. Diagrama Download do Arquivo. (Própria).

Logo abaixo, na Figura 18 é demonstrado código fonte do arquivo 'RequisicaoWEB.exe' responsável por efetuar a requisição para *Download* ao Servidor *Web* por meio do Endereço 'http://localhost:8080/axis/Assinador_ICP-Brasil.rar, após a conclusão do *Download*, é realizado uma verificação Local, para identificar a onde foi armazenado o Arquivo baixado. Após a identificação do local do arquivo, o mesmo será extraído para a raiz do endereço local 'C:'.

```
SET ARQUIVO=http://localhost:8080/axis/Assinador_ICP-Brasil.rar

cls
color 1f

if exist "c:\Program Files (x86)\WinRAR\Rar.exe" (
"C:\Arquivos de Programas (x86)\WinRAR\Rar.exe" -df x -y "%Userprofile%\Downloads\Assinador_ICP-Brasil.rar" *.* c:\
)
else (
"C:\Arquivos de Programas (x86)\WinRAR\Rar.exe" -df x -y "%Userprofile%\Meus Documentos\Assinador_ICP-Brasil.rar" *.* c:\
)
else (
"C:\Arquivos de Programas (x86)\WinRAR\Rar.exe" -df x -y "%Userprofile%\Desktop\Assinador_ICP-Brasil.rar" *.* c:\
)
else (
"C:\Arquivos de Programas (x86)\WinRAR\Rar.exe" -df x -y "%Userprofile%\Meus Documentos\Downloads\Assinador_ICP-Brasil.rar" *.* c:\
)
else (
"c:\Program Files\WinRAR\rar.exe" -df x -y "%Userprofile%\Downloads\Assinador_ICP-Brasil.rar" *.* c:\
)
else (
"c:\Program Files\WinRAR\rar.exe" -df x -y "%Userprofile%\Meus Documentos\Assinador_ICP-Brasil.rar" *.* c:\
)
else (
"c:\Program Files\WinRAR\rar.exe" -df x -y "%Userprofile%\Desktop\Assinador_ICP-Brasil.rar" *.* c:\
)
else (
"c:\Program Files\WinRAR\rar.exe" -df x -y "%Userprofile%\Meus Documentos\Downloads\Assinador_ICP-Brasil.rar" *.* c:\
)
```

Figura 18. Código Fonte Requisição do arquivo ao Servidor e Verificação Local (Própria).

A Figura 19 apresenta o instante em que é executado o Assinador Digital ICP - Brasil, onde todas as funcionalidades da aplicação são executadas em segundo plano, gerando assim um arquivo Log, contendo todas as Informações pertinentes para a concretização da assinatura de um Documento. Lembrando que as informações inseridas no arquivo Log.txt são inseridas no navegador no momento da execução.

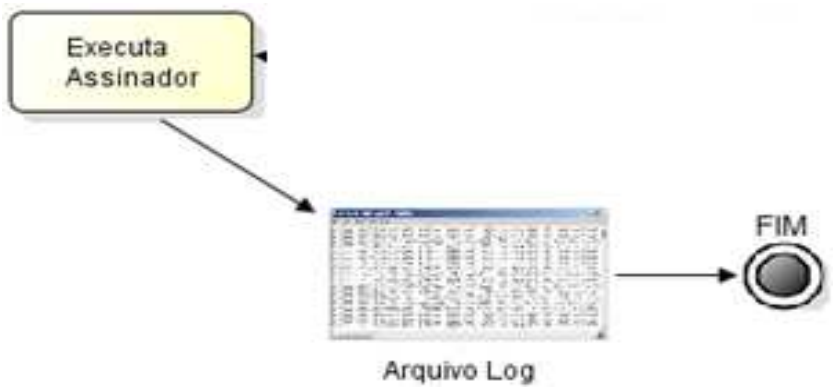


Figura 19. Diagrama Executar Assinador e Gerar Arquivo Log. (Própria).

4.3 Alterações Realizadas no Projeto Inicial

Para o desenvolvimento do projeto foi necessário realizar algumas alterações no Assinador Digital ICP – Brasil. Abaixo são destacadas as alterações realizadas no projeto.

- Desativado Parte Gráfica
- Criado Nova Classe para Estabelecer a conexão entre as duas plataformas
- Função Para gerar o Arquivo Log.txt
- Atribuindo Valores a Variáveis.
- Selecionando Principais Informações necessárias para Realizar a Assinatura.

4.4 Plugin para Assinador

Por ser uma linguagem de programação interpretada para navegadores *Web*, e que facilita a execução de comandos do cliente, ou seja, em termos do navegador e não do servidor *web*. A linguagem *JavaScript* foi utilizada para realizar essa comunicação entre a pagina *Web* com o assinador, onde o cliente buscara o arquivo, o endereço desse arquivo será armazenado em uma variável e enviado para o assinador, destacando-se a função ‘RUN’ a qual utilizei para realizar a chamada da aplicação executável (Assinador Digital ICP - Brasil) de dentro do computador local. Passando por parâmetro o endereço da aplicação executável. Ilustrado na Figura 20.

```
var inicia = function(pathArquivo){
        getFile();
        var app = new ActiveXObject("WScript.shell");
        var comando = "C:\\Users\\Marquinho\\Desktop\\Fonts\\app\\dist\\app.jar " + pathArquivo;

        //app.run(comando);
        try{
            app.run(comando)
            }catch(e){
                console.log("Erro 1 "+e.message);
                try{
                    //pegar o arquivo no servidor
                    var reqArquivo = new ActiveXObject("Microsoft.XMLHTTP");
                    reqArquivo.open("GET","localhost:8080/axis/app.jar", false);
                    reqArquivo.send();

                    app.run(comando);

                }catch(e){
                    console.log("Erro 2 "+e.message);

                }
            }
```

Variavel 'caminho' recebendo o endereço do Arquivo App.jar

Função RUN

Figura 20. Código para Envio do endereço do Arquivo e Execução da aplicação. (Própria).

Para o andamento do projeto foi necessário realizar algumas alterações no código fonte do Software de Assinatura digital ICP – Brasil que foi desenvolvido na *Integrated Development Environmen* (IDE) NetBeans 7.3.1 para atender as devidas exigências do projeto. Sendo desabilitada toda a parte gráfica da aplicação, para que a mesma fosse executada em modo *background*.

Sendo criada uma nova classe ‘funcoes’ para facilitar a comunicação entre a aplicação e o Assinador, onde a mesma trabalha como uma conexão entre a aplicação web, com o assinador. Como ilustrado na Figura abaixo 21.

```
public class funcoes {
    static String caminho;

    public static String getCaminho() {
        return caminho;
    }
```

Figura 21. Função para conexão entre aplicação Web e Assinador Digital ICP-Brasil. (Própria).

A classe “Funcoes” fica responsável por receber o endereço do arquivo que será assinado e encaminhá-lo para os devidos lugares. De dentro do assinador é resgatado esse endereço que esta sendo passado por parâmetro, através da String args[0]. Ilustrado na Figura 22.

```
        funcoes.gerarLog("Inicilizado");
         new Thread(new Runnable() {
             @Override
             public void run() {
                 Main.initICPBrasil();
             }
         }).start();
         if (args.length == 0) {
             Main.startSigner();
         }
         else{
             funcoes.setCaminho(args[0]);
             Main.startSigner();
         }
    }
```

Função SetCaminho

Figura 22. Código para pegar endereço passado pela aplicação Web. (Própria).

Apos obter o endereço do arquivo a ser assinado, o mesmo é atribuído ao Item tfFiles, responsável em armazenar o endereço do arquivo selecionado, sendo assim o assinador já possui o endereço do arquivo para ser assinado. Não sendo mais necessário buscar o arquivo por meio do botão da aplicação.

Para realizar a assinatura, é necessário realizar a instalação de alguns certificados locais. Com os certificados já instalados, o signersList.setSelectedIndex(); selecionaria um dos certificados, de acordo com o valor atribuído para ele, por padrão será atribuído sempre o valor '0', selecionando sempre o primeiro certificado da lista signersList. Ilustrado na Figura 23.

.

```
//funcoes.gerarLog(signersList.setSelectedIndex(0));
this.chooser = owner.makeChooser();
initComponents();
this.updateFilesField(this.owner.getFiles());
this.tfFiles.setText(funcoes.getCaminho());
funcoes.gerarLog(funcoes.getCaminho());
File arquivo = new File(funcoes.getCaminho());

chooser.setSelectedFile(arquivo);
this.owner.setFile(arquivo);
signersList.setSelectedIndex(0);
```

Função GetCaminho

Função Gerar Log

SignersList- 1 Posição

Figura 23. Código para atribuir valores a algumas Propriedades. (Própria).

A função ‘gerarLog’ é responsável por gerar um log e armazenar em um arquivo TXT, todo o processo de assinatura, dês da inicialização da aplicação, o diretório do arquivo selecionado, o primeiro certificado encontrado na lista e todas as informações pertinentes a esse certificado.

```
public static void gerarLog(String msg){
  File arquivo = new File( "c:\\log\\log.txt" );
   try {
       FileWriter fw = new FileWriter( arquivo, true );
       BufferedWriter bw = new BufferedWriter( fw );
       String texto = "";

       DateFormat dateFormat = new SimpleDateFormat("dd/MM/yyyy HH:mm:ss");
       Date date = new Date();

       texto += dateFormat.format(date)+" -> "+msg;
       bw.newLine();
       bw.write(texto);
       bw.newLine();

       bw.close();
       fw.close();
```

Figura 24. Função para Gerar Log. (Própria).

Através da pagina *web*, é possível selecionar o arquivo que se deseja assinar e posteriormente sendo carregado o seu endereço, ao clicar no botão “Assinar Documento” é executada a função RUN do *JavaScript* sendo responsável por executar o *software* ‘Assinador Digital ICP – Brasil’ passando por parâmetro o endereço do arquivo para a aplicação.

Na função “Funções” é criado uma variável do tipo String, a qual recebera através da função SetCaminho (args[0]); o endereço do arquivo a ser assinado.

Com o endereço do arquivo já atribuído a aplicação, SignersList.setSelectedIndex(0) selecionara sempre o primeiro certificado que encontrar na lista, sendo percorrido todo o processo para concretizar a assinatura de um Documento.

4.4.1 Tecnologias do Projeto

Para a elaboração do projeto, foi utilizado algumas tecnologias. Dentre elas:

- Assinador Digital ICP - Brasil – Desenvolvido na Linguagem de Programação Java, foi utilizado como base para a elaboração do projeto.
- Linguagem de Programação JavaScript - Utilizada para realizar a comunicação entre ambas as Plataformas (*Web* e *Desktop*) passando por parâmetro o endereço do arquivo que se deseja assinar e realizando a execução do Assinador digital ICP – Brasil.
- HTML – Linguagem Utilizada para desenvolver a Tela Principal e realizar a busca do arquivo na maquina Local. Exibindo o arquivo log.txt em momento de Execução.
- Apache *TomCat* – Servidor *Web* Utilizado para armazenar o Assinador Digital.
- *Framework* Apache Axis – Utilizado para a Construção do *Web Services*.

4.4.2 Serviço *Web*

Segundo ROMAN et al. (2005, apud AUSTIN et al., 2002). Um serviço *Web* é uma aplicação identificada por um URI, cujas interfaces e ligações são definidas, descritas e localizadas por artefatos que utilizam a linguagem XML. Um serviço *Web* deve ser capaz de interagir com outras aplicações através da troca de mensagens XML utilizando os protocolos de comunicação padrão atualmente disponíveis na *Internet*. (tradução nossa).

> "Os Serviços *web* representam entidades computacionais capazes de fornecer acesso a serviços que, por sua vez, fornecem algum valor em um domínio". (ROMAN et al., 2005). (tradução nossa).

A tecnologia de serviços *Web* traz consideráveis benefícios para o desenvolvimento de aplicações, uma vez que propicia a agilidade requerida pelas empresas frente às rápidas mudanças no ambiente de negócios. Uma das principais vantagens do uso dos serviços *Web* está na sua elevada interoperabilidade, obtida graças à adesão a protocolos e padrões amplamente difundidos na *Web*, como por exemplo, SOAP, HTTP, XML, entre outros.

Basicamente o Servidor *Web* é Um programa de computador responsável por aceitar pedidos HTTP de clientes, geralmente os navegadores, e servi-los com respostas HTTP, incluindo opcionalmente dados, que geralmente são páginas *web*, tais como documentos HTML com objetos embutidos (imagens, etc.).

O navegador *Web* utiliza-se do protocolo HTTP para “chamar” uma aplicação ou applet Java em um servidor *Web*. Ilustrado na Figura 25.

Figura 25. Conexão de um cliente através de servidor Web. (Devmedia, Oracle 9i - Conexões de rede).

CAPITULO 5 – TESTES E RESULTADOS

4.5 Testes

Inicialmente foi realizado a passagem de parâmetro do *javaScript* para o assinador, sem a necessidade de selecionar o arquivo, pois o mesmo já havia sido atribuído por parâmetro. No entanto não foi obtido os resultados esperados, pois a Lista de certificados revogados que estava armazenada no repositório: http://www.lsitec.org.br/repositorio/LSITEC.PEM.P7C, foi alterado para o repositório no endereço: http://www.lsitec.org.br/repositorio/Olds/Backup-CRL-20140618/LSITEC.PEM.P7C, sendo assim não foi possível concluir o processo de assinatura, sendo fundamental essa cadeia de certificados para concluir o processo de assinatura.

Com isso foi realizado um mapeamento do processo de assinatura, sendo inserido em um arquivo Log.TXT todo o processo da assinatura, desde a inicialização da aplicação, até o momento de confirmar a assinatura.

Sendo realizada a instalação de dois certificados para teste. Para que a aplicação sempre selecione a primeira opção disponível na lista de certificado. Ilustrado na Figura 26 e 27.

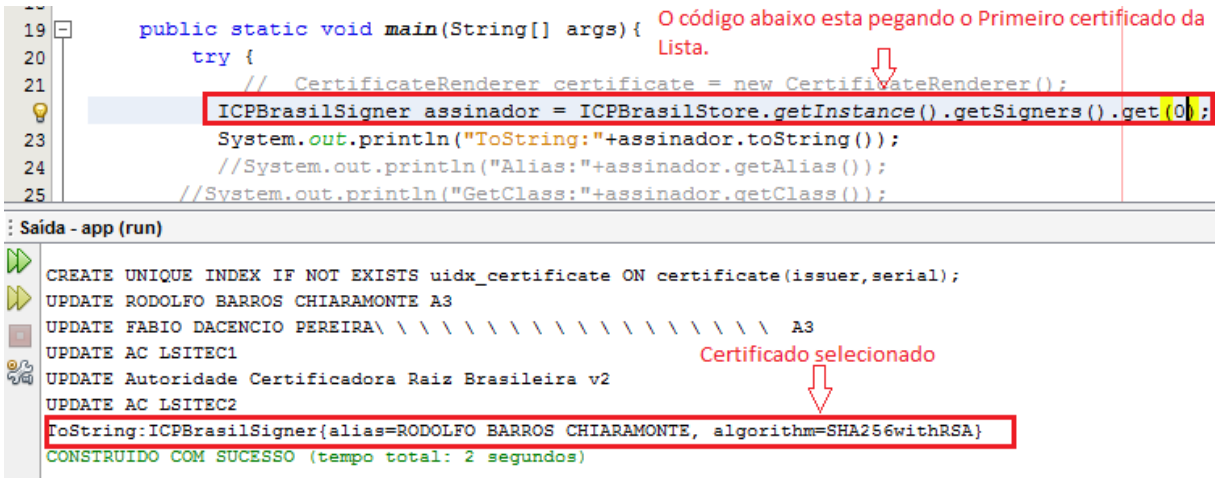
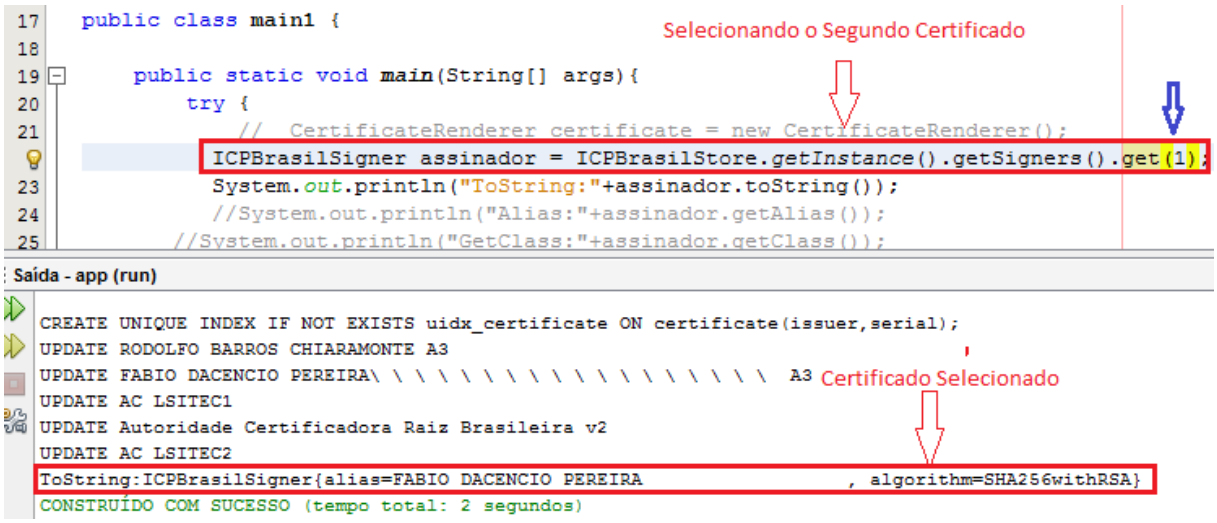


Figura 26. Selecionando o Primeiro certificado. (Própria).




```
17  public class main1 {
18
19      public static void main(String[] args){
20          try {
21              //  CertificateRenderer certificate = new CertificateRenderer();
                ICPBrasilSigner assinador = ICPBrasilStore.getInstance().getSigners().get(1);
23              System.out.println("ToString:"+assinador.toString());
24              //System.out.println("Alias:"+assinador.getAlias());
25          //System.out.println("GetClass:"+assinador.getClass());
```

```
CREATE UNIQUE INDEX IF NOT EXISTS uidx_certificate ON certificate(issuer,serial);
UPDATE RODOLFO BARROS CHIARAMONTE A3
UPDATE FABIO DACENCIO PEREIRA\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ A3
UPDATE AC LSITEC1
UPDATE Autoridade Certificadora Raiz Brasileira v2
UPDATE AC LSITEC2
ToString:ICPBrasilSigner{alias=FABIO DACENCIO PEREIRA                    , algorithm=SHA256withRSA}
CONSTRUÍDO COM SUCESSO (tempo total: 2 segundos)
```

Figura 27. Selecionando o Segundo Certificado. (Própria).

4.6 Resultados

Dentre os resultados Destaca-se:

- Comunicação da Pagina Web com o Assinador ICP – Brasil
- Processo De assinatura Sendo Realizado em Modo *Background.*
- Não Foi possivel Concretizar a Assinatura do Documento
- Aplicação Limitada ao Internet Explorer
- Informações Armazenadas em um Arquivo Log

Todo o processo de assinatura esta sendo executado localmente em modo *background*, sendo necessário que o cliente apenas selecione o arquivo e clique no botão “Assinar Documento” e todo o processo será executado em questões de Segundos.

Como a assinatura não esta sendo realizada devido a alteração no repositório que contem a lista de certificados revogados, foi gerado um arquivo log, obtendo todos os processos da assinatura, inserindo no navegador em momento de

execução todos os passos que esta sendo realizado naquele instante.

Obtendo Informações do Tipo:

- Nome do Assinador
- Há *Hash* do Certificado
- Para quem o certificado foi Emitido
- Chave Publica e a Quantidade de Bits que Compõem essa Chave
- Data de Validade do Certificado dentre outras informações

Ilustrado na Figura 28 e 29

```
1
2  20/11/2015 01:25:16 -> Inicilizado
3
4  20/11/2015 01:25:17 ->  O assinador é: ICPBrasilSigner{alias=RODOLFO BARROS CHIARAMONTE, algorithm=SHA256withRSA}
5
6  20/11/2015 01:25:17 ->  O caminho para o Arquivo  é: C:\Users\Marquinho\Desktop\marcos.txt
7
8  20/11/2015 01:25:17 ->  A chave do Assinador é: null
9
10 20/11/2015 01:25:17 ->  HashCode: 73887986
11
12 20/11/2015 01:25:17 ->  Get Alias: RODOLFO BARROS CHIARAMONTE
13
14 20/11/2015 01:25:17 ->  Classe do Certificado: class compsi.icpbrasil.ICPBrasilSigner
15
16 20/11/2015 01:25:17 -> certificado: [
17 [
18   Version: V3
19   Subject: CN=RODOLFO BARROS CHIARAMONTE, OU=AC LSITEC2, OU=Certificados de Testes AC LSITEC2, O=ICP-Brasil, C=BR
20   Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11
21
22   Key:  Sun RSA public key, 2048 bits
23   modulus: 20435979666527065203108073904092127545805309893719083433451219445891558373693636916697731806676632974174
24            08298726116120235571114649144814438278493734142176106571987497988680930406310001817524704513563552015560
25            74428438825506488409460757470309245185714007941354081545449316614685917398720718677608024546780409456408
26            07762295690140671667477703412596309617318049112283022547991928388713337697864781659221804562168182655975
27            21460280460587258896604456344659011151726876167616396208414656129757672027022616274682868263911505081600
28            40618345936770682524596058375562259295438319500091540190668838914884538393766602703102189657
29   public exponent: 65537
30   Validity: [From: Fri Feb 03 10:29:05 BRST 2012,
31               To: Mon Feb 02 10:29:05 BRST 2015]
32   Issuer: CN=AC LSITEC2, OU=Certificados de Testes AC LSITEC2, O=ICP-Brasil, C=BR
33   SerialNumber: [    0a]
```

Figura 28. Log de Saida. (Própria).

A Tabela 1 apresenta parte das principais informações geradas pelo arquivo Log, expondo uma breve e objetiva explicação de cada campo, visando uma melhor compreensão daqueles que possam apreciar o presente projeto.

Tabela 1. Informações do Log de Saída. (Própria).

CAMPO	EXPLICAÇÃO
C:\Users\Marquinho\Desktop\marcos.txt	Endereço do Arquivo enviado por parâmetro para ser assinado.
HashCode: 73887986	Apresenta o Código de *Hash* do Certificado
Alias: RODOLFO BARROS CHIARAMONTE	O nome para quem foi emitido o Certificado
Class: class compsi.icpbrasil.ICPBrasilSigner	Classe que contem os certificados
Signature Algorithm: SHA256withRSA	Algoritmo de *criptografia* de dados que foi utilizado no certificado
Key: Sun RSA: public key, 2048 bits	Chave RSA Publica utilizada na *criptografia* do certificado, composta por 2048 Bits.
Validity: [From: Fri Feb 03 10:29:05 BRST 2012, To: Mon Feb 02 10:29:05 BRST 2015]	Validade do Certificado entre 03 de fevereiro de 2012, á 02 de fevereiro de 2015.
SerialNumber: [0a]	Numero de Série do Certificado.

```
35  Certificate Extensions: 9
36  [1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
37  AuthorityInfoAccess [
38    [
39     accessMethod: caIssuers
40     accessLocation: URIName: http://www.lsitec.org.br/repositorio/LSITEC.pem.p7c
41  ,
42     accessMethod: ocsp
43     accessLocation: URIName: http://ocsp.lsitec.org.br
44  ]
45  ]
46
47  [2]: ObjectId: 2.5.29.35 Criticality=false
48  AuthorityKeyIdentifier [
49  KeyIdentifier [
50  0000: C6 D0 50 49 D9 C9 67 95   58 DC D2 E9 37 93 A0 12  ..PI..g.X...7...
51  0010: 06 7E EF 9B                                        ....
52  ]
53  ]
54
55  [3]: ObjectId: 2.5.29.19 Criticality=false
56  BasicConstraints:[
57    CA:false
58    PathLen: undefined
59  ]
60
61  [4]: ObjectId: 2.5.29.31 Criticality=false
62  CRLDistributionPoints [
63    [DistributionPoint:
64       [URIName: http://www.lsitec.org.br/repositorio/LSITEC2.pem.crl]
65  ]]
```

Figura 29. Log de Saída. (Própria).

A Tabela 2 visa dar continuidade nas principais informações geradas a partir do arquivo Log apresentado na Figura 29, destacando-se algumas informações que não foram apresentadas na Tabela 1.

Tabela 2. Informações do Log de Saída. (Própria).

CAMPO	EXPLICAÇÃO
accessLocation: URIName: http://www.lsitec.org.br/repositorio/LSITEC.pem.p7c	Local para Acesso aos Certificados utilizando o endereço: http://www.lsitec.org.br/repositorio/LSITEC.pem.p7c
accessLocation: URIName: http://ocsp.lsitec.org.br	Local para Acesso aos certificados Utilizando o endereço http://ocsp.lsitec.org.br
DistributionPoint: URIName: http://www.lsitec.org.br/repositorio/LSITEC2.pem.crl	Ponto de distribuição dos certificados através do endereço: http://www.lsitec.org.br/repositorio/LSITEC2.pem.crl

Por fim, destaca-se na Figura 30, uma pequena apresentação da aplicação implementada, onde nota-se que a mesma já contém as informações importadas do arquivo Log, como seus respectivos botões de Busca, para se selecionar o arquivo, e o de ‘Assinar Documento’, para realizar todo o processo de assinatura de um documento.

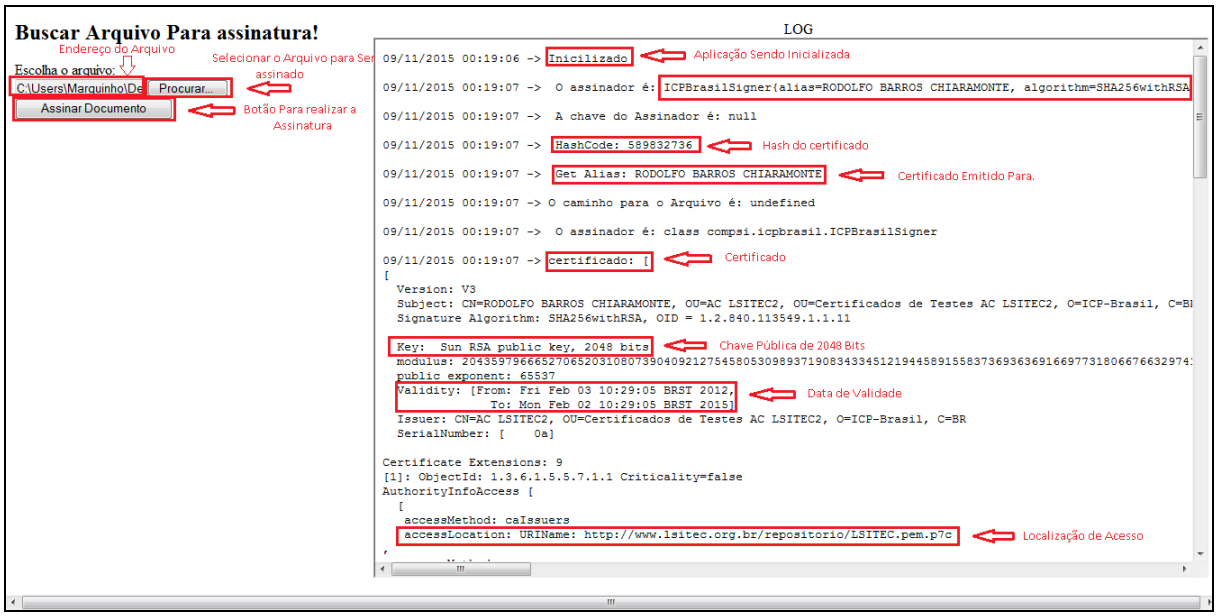


Figura 30. Aplicação de Assinatura Digital – Web. (Própria).

5.3 Limitações

- Não Foi possível Concretizar a Assinatura do Documento
- Aplicação Limitada ao Internet Explorer
- Aplicação testada somente em Ambiente Windows

5.4 Desafios

- Estudo Da API Assinador Digital ICP – Brasil
- Estudo Linguagem de Programação JavaScript.

- Alteração do Código Fonte do Assinador.
- Servidor Web TomCat

CONCLUSÕES

Existem varias tecnologias no mercado destinadas a assegurar a Confidencialidade, Integridade e a Disponibilidade das informações trafegadas pela rede, no entanto a mais disseminada é a do sistema de assinaturas e certificados digitais que são baseados na *criptografia* de chaves publicas, destacando-se que o mesmo possui um órgão regulamentador sério e eficaz, á Infraestrutura de Chaves Pública Brasileira (ICP – Brasil) que tem por objetivo estabelecer fundamentos técnicos e metodológicos de um sistema de certificação digital. Sendo o Instituto Nacional de Tecnologia da Informação responsável por regulamentar minuciosamente cada detalhe no processo de assinatura, trazendo assim uma maior segurança e tranqüilidade para os usuários.

Porém mesmo com toda essa regulamentação e cuidado, existem pessoas o qual se sentem inseguras quando são instadas a transacionar e se comunicar em ambientes que não fornecem completas condições de proteção aos seus interesses, bens e privacidade de suas informações. Pensando nisso, o presente trabalho visou à oportunidade de desenvolver um *Plugin* de assinatura digital, a qual realizara todo o processo de assinatura localmente, não sendo necessária a transição das informações do cliente na *Web*. Enfatizando a utilização do 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) como base.

Conclui-se que disponibilizar uma aplicação web com esse porte, poderá proporcionar uma maior segurança e tranqüilidade nas pessoas que as utilizam, pois todo o processo será concentrado no seu computador local. De modo que documentos eletrônicos possam ser assinados de forma segura, garantindo sua validade jurídica.

Como trabalho futuro, sugere-se a correção do problema em função dos certificados revogados terem sido alterados de diretórios.

REFERÊNCIAS BIBLIOGRÁFICAS

BARRA, Marcello Cavalcanti. Infra-estrutura de chaves públicas brasileira (ICP - BRASIL) e a formação do estado eletrônico. 2006. 161 f. Dissertação (Mestrado em Sociologia)-Universidade de Brasília.

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.

CARDOSO, Fernando Henrique; GREGORI, José; TAVARES, Martus; SARDENBERG, Ronaldo Mota; PARENTE, Pedro. MEDIDA PROVISÓRIA No 2.200-2, DE 24 DE AGOSTO DE 2001. Brasília, 2001. Disponível em: < http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm >. Acessado em: 28 Abr 2015.

CARVALHO, Italo Rezende Ferreira. Segurança da Informação: Um instrumento para avaliação do plano de continuidade do Negocio aplicado em uma Organização Pública. 2011. Tese (Monografia em Ciências da Computação)-Universidade Federal de Lavras, Minas Gerais, 2011.

CORREIOS. Certificados digitais. 2015. Disponível em: < http://www.correios.com.br/para-voce/compra/certificados-digitais >. Acessado em: 29 Abr 2015>.

EDUCA. O que são Pluguins. 2009. Disponível em: http://www.oieduca.com.br/artigos/nunca-e-tarde-para-aprender/o-que-sao-plugins.html acesso em: 29 Mar. 2015.

FERREIRA, Fernando Nicolau Freitas**. Segurança da Informação.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2003.

ICP-Brasil, ITI Glossário. "Instituto Nacional de Tecnologia da Informação."

INFORMAÇÃO, Instituto Nacional de Tecnologia. Sobre Carimbo de Tempo. Brasília, 2012. Disponível em: http://www.iti.gov.br/perguntas-frequentes/1747-carimbo-de-tempo Acesso em: 27 Mar. 2015.

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.

ITI, ITI LANÇA VERIFICADOR DE CONFORMIDADE DO PADRÃO DE ASSINATURA DIGITAL ICP-BRASIL, disponível em: <http://www.iti.gov.br/noticias/indice-de-noticias/4690-iti-lanca-verificador-de-conformidade-do-padrao-de-assinatura-digital-icp-brasil>, acessado em Jun. de 2015.

LAUREANO, Marcos Aurelio Pchek ; MORAES, Paulo Eduardo Sobreira. SEGURANÇA COMO ESTRATÉGIA DE GESTÃO DA INFORMAÇÃO. 2005. Revista Economia & Tecnologia – ISSN 1415-451X Vol. 8 – Fascículo 3 – P. 38-44.

LAUREANO, Marcos Aurelio Pchek. Gestão de segurança da informação. **Publicado em**, v. 1, n. 06, 2005.

MARCACINI, Augusto Tavares Rosa. **Direito e Informática: uma abordagem jurídica sobre a Criptografia**. São Paulo, 2010.

MARCIANO, João Luiz Pereira. Segurança da informação: uma abordagem social. 2006. 212 f. Tese (Doutorado em Ciência da Informação)-Universidade de Brasília, Brasília, 2006.

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

NEWS, E-commerce. China, Índia e Brasil são os países que mais sofrem ataques. 2010. Disponível em: http://ecommercenews.com.br/noticias/crimes-noticias-3/china-india-e-brasil-sao-os-paises-que-mais-sofrem-ataques Acesso em: 24 Mar. 2015.

ROCHA, Paulo Cesar Cardoso. Segurança da Informação – Uma questão não apenas Tecnológica. Curso (Especialização em Gestão da Segurança da Informação e Comunicações)-Universidade de Brasília, Brasília, 2008.

SILVA, Nelson; RAMOS, Thiago Acórdi; CUSTÓDIO, Ricardo Felipe. Carimbos do Tempo Autenticados para a Preservação ao por Longo Prazo de Assinaturas Digitais. Laboratório de Segurança em Computação (LabSEC) - Universidade Federal de Santa Catarina (UFSC). Florianópolis – SC. Disponível em: http://www.peotta.com/sbseg2011/resources/downloads/sbseg/90812.pdf Acesso em: 25 Mar. 2015.

TERADA, Routo. Segurança de dados: Criptografia em rede de computador. São Paulo: Blucher, 2008. 2 edição revista e ampliada.

TOGNOLI, Éttore Leandro. Verificador de Certificados e Assinaturas ICP-Brasil em Java. Bacharelado em Ciência da Computação – Fundação de Ensino “Eurípides

Soares da Rocha”. Marília, 2012.

TRINTA, Fernando Antonio Mota; MACÊDO, Rodrigo Cavalcanti. Um Estudo sobre Criptografia e Assinatura Digital. Universidade Federal de Pernambuco. Univerdade Federal de Pernambuco, Setembro, 1998.

VIEIRA, Sergio Santos. Assinatura Digital de Documentos. Graduação Universidade Candido Mendes Pós-Graduação "Lato Sensu" AVM Faculdade Integrada. Rio de Janeiro, 2012.

WEBER, Raul Fernando. Criptografia contemporânea. In: **VI Simpósio de Computadores Tolerantes a Falhas**. 1995. p. 7-32.

WIKIPEDIA. Assinatura Digital. 2015. Disponível em: http://pt.wikipedia.org/wiki/Assinatura_digital acesso em 25 Mar. 2015.

WIKIPEDIA. Cifra de substituição. 2014. Disponível em: http://pt.wikipedia.org/wiki/Cifra_de_substitui%C3%A7%C3%A3o Acesso em: 29 Mar. 2015.

ROMANA, Dumitru; KELLERA, Uwe; LAUSENA, Holger; BRUIJNA, Jos; LARA, Ruben; STOLLBERGA, Michael; POLLERESA, Axel; FEIERA, Cristina; BUSSLERB, Cristoph; FENSELA, Dieter. Web Service Modeling Ontology. Digital Enterprise Research Institute Innsbruck (DERI Innsbruck), University of Innsbruck, Austria, 2005; Digital Enterprise Research Institute (DERI), Galway, Ireland, 2005. Disponível em: https://vsr.informatik.tu-chemnitz.de/edu/2011/webe-seminar-ws/material/12/wsmo.pdf. Acesso em: 05 DEZ. 2015.