Assinatura Digital: A validade dos Certificados Digitais com ênfase no Carimbo do Tempo

Cristiano Andreatta[1], Sylvio Andre Garcia Vieira[1]

[1]Sistemas de Informação - Centro Universitário Franciscano (UNIFRA)
Rua dos Andradas 1614 – 97.010-032 – Santa Maria – RS - Brasil

{cristiano.joiaa@gmail.com,sylvio@unifra.br}

Abstract. *This paper proposes the use of the certificates for the verification of the digital signature for electronic documents, giving greater security in electronic transactions through the Stamp of Time. The prototype was developed using the Java programming language and software development methodology was the ICONIX, following the patterns of certificates of ICP-Brazil.*

Resumo. Este trabalho propõe o uso de certificados para a verificação da assinatura digital de documentos eletrônicos, buscando dar uma maior segurança nas transações eletrônicas por meio do Carimbo de Tempo. O protótipo foi desenvolvido utilizando a linguagem de programação Java, e a metodologia de desenvolvimento de software foi o ICONIX, seguindo os padrões de certificados da ICP-Brasil.

1. Introdução

Atualmente observa-se o uso cada vez maior dos meios eletrônicos no ambiente em que vivemos. Usa-se a internet para realizar todos os tipos de transações eletrônicas, aumentando assim a necessidade e a busca por segurança na troca de informações. Nesse cenário, o papel vem perdendo espaço, dando lugar a um novo tipo de registro de informações, denominado documentos eletrônicos. Com a utilização dos documentos eletrônicos, reduziram-se os gastos e o tempo que um processo demorava a ser realizado, garantindo assim proteção nas transações e uma maior otimização nos processos, utilizando o método de assinatura digital [Silva 2011].

Com a necessidade de comprovar a integridade, confiabilidade e não repúdio dos documentos eletrônicos surge uma técnica de assinar documentos virtuais, a assinatura digital [Pinheiro 2011]. A assinatura digital consiste em um método de criptografia, que pode ser aplicada em um determinado tipo de arquivo. Seu uso se da através de chaves públicas e privadas e se fundamenta na criptografia assimétrica. Para a criação de uma assinatura digital confiável, somente é possível através do uso de certificados digitais, que são um conjunto de dados de computador gerado por uma autoridade certificadora, e que tem relação entre uma chave criptográfica e uma pessoa física, jurídica ou de máquina. Contudo, as assinaturas digitais acabam perdendo sua validade por enfraquecimentos de algoritmos criptográficos ou pelo comprometimento da chave privada do signatário [Silva 2011].

Este estudo trabalha com políticas de assinatura voltada aos padrões da ICP-Brasil (Infraestrutura de Chaves Públicas Brasileiras). Visando dar uma maior segurança na troca de informações, é utilizada a técnica de Carimbo de Tempo, que serve para garantir a data e a hora da assinatura digital de documentos eletrônicos em sincronia com a hora legal brasileira (Hora Legal Brasileira - HLB), assim garantindo a validade das assinaturas digitais por um tempo necessário.

A Seção 2 deste trabalho apresenta um embasamento teórico sobre os tipos de criptografias envolvidas, as características da assinatura digital, padrões da certificação digital e a segurança das informações utilizando o carimbo de tempo. Logo após o embasamento teórico será apresentada a Seção 3, são apresentados os trabalhos realizados por outros autores sobre a certificação digital e seus procedimentos. A Seção 4 apresentará a metodologia usada, a ICONIX. A Seção 5 tratará do desenvolvimento do trabalho, a Seção 6 apresentará os resultados obtidos e por fim a Seção 7 apresentará a conclusão e a Seção 8 apresentará as referências bibliográficas utilizadas para a realização deste trabalho.

1.2 Justificativa

Com a crescente utilização dos meios eletrônicos, a assinatura digital traz tecnologia e procedimentos que reduzem a burocracia e o fluxo de documentos em empresas e instituições de todos os segmentos. Se, por um lado, assinar documentos reduz gastos e tempo, por outro, o processo de assinatura digital ainda exige que o usuário tenha acesso a um computador para que possa realizar a assinatura. Para que a assinatura digital seja utilizada, torna-se necessário ter também um certificado digital. Este é um documento eletrônico que tem por finalidade garantir a proteção nas transações online e a troca virtual de documentos. Assim, a assinatura digital se propõe a dar uma maior agilidade nos processos, buscando alta produtividade e uma maior segurança dos documentos eletrônicos.

A certificação digital vem ajudando a reduzir impactos causados pelo uso excessivo de papel, água, energia e etc. Usar a tecnologia da certificação digital para substituir documentos em papel pelos eletrônicos contribui para a sustentabilidade ambiental.

1.3 Objetivos Gerais

Este trabalho tem como objetivo implementar uma ferramenta para assinar digitalmente documentos eletrônicos e verificar junto ao Observatório Nacional a hora e a data, utilizando o método do Carimbo do Tempo, seguindo os requisitos de segurança e os padrões da ICP-Brasil.

1.4 Objetivos Específicos

- Definir metodologia para desenvolvimento do software;
- Identificação dos requisitos;
- Analisar trabalhos relacionados;
- Desenvolvimento do *software* gerador de certificados digitais e do carimbo de tempo;

- Implementar ferramenta.
- Teste;
- Validação

2 Referencial Teórico

O Referencial Teórico permite verificar o estado do problema a ser pesquisado, sobe o aspecto técnico e sobre estudos e pesquisas realizadas no decorrer do trabalho. Nessa Seção será abordado sobre as referidas pesquisas, características e requisitos abordados para realizar a assinatura digital.

2.1 Criptografia

A criptografia tem como objetivo codificar uma série de informações para que os usuários troquem com segurança seus dados entre si [Alecrim 2009].

A criptografia pode ser dividida em dois tipos: Criptografia Simétrica e Assimétrica, as quais são as mais relevantes e atendem os requisitos de segurança para o uso da certificação digital.

2.1.1 Criptografia Assimétrica ou de Chave Pública

A criptografia assimétrica envolve algoritmos que possuem um par de chaves, ou seja, ela trabalha com duas chaves diferentes, uma para cifrar e outra decifrar uma mensagem. Elas se relacionam matematicamente e a segurança depende do número de bits das chaves.

O que a chave pública codifica, só pode ser decodificada com a chave privada e vice-versa. Então, quando uma chave codifica, a outra decodifica. A chave de cifrar consiste em uma chave pública, quando o utilizador pretende decifrar alguma mensagem, assim utilizando uma chave privada. A chave de decifrar consiste eu uma chave secreta, onde apenas o utilizador poderá decifrá-la, na Figura 1 é mostrado como é feita a codificação e a decodificação com o principio da criptografia de chave Assimétrica [Mamede 2006].

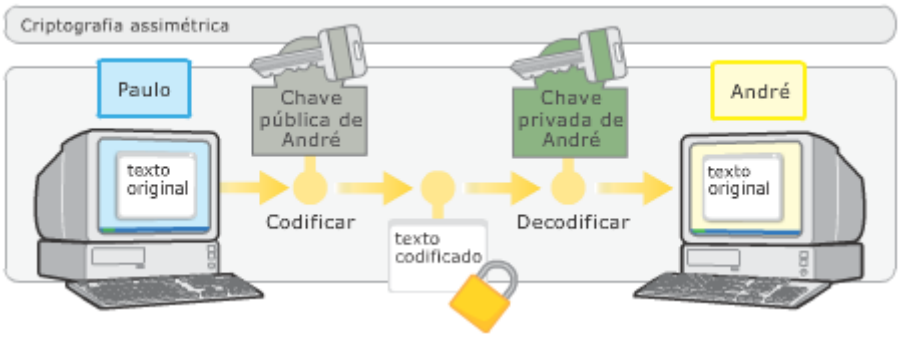

Figura 1 - Codificação e Decodificação com Chave Assimétrica [RIBEIRO 2008].

2.1.2 Criptografia Simétrica ou de Chave Privada

Conhecida como um método criptográfico convencional, a criptografia simétrica, mostra-se como o mais simples e o primeiro método a utilizar técnicas de segurança na troca de informações. Sua principal característica está na utilização de apenas uma chave para autenticar a mensagem, assegurando assim, a integridade do mesmo. Seu

funcionamento se da através da transformação de um texto em uma mensagem cifrada, para isto, utiliza-se uma chave secreta e o método de decriptar à mensagem, o qual irá trazer o texto na sua forma original, na Figura 2 é mostrado como é feita a codificação e a decodificação com o principio da criptografia de chave Simétrica [Cavalcante 2004].

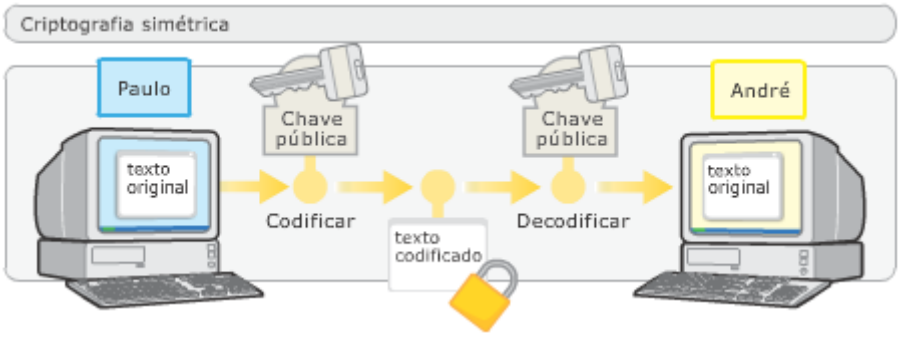

Figura 2 - Codificação e Decodificação com Chave Simétrica [RIBEIRO 2008].

2.2 Assinatura Digital

A assinatura digital consiste em uma tecnologia que tem como principal característica, garantir a integridade e autenticidade dos documentos eletrônicos. Ela utiliza o método de criptografia, sendo aplicada em um determinado tipo de arquivo, ou seja, ela permite certificar que a mensagem não foi alterada e que a mesma foi assinada por quem possui a chave criptográfica (chave privada) [Justiça 2013].

A assinatura digital faz uso de chaves públicas e privadas utilizando o método de criptografia assimétrica e a função *hashing*, para obter uma mensagem digital. [Floriano 2007].

Para verificar a assinatura usa-se uma chave pública, disponibilizada no próprio documento sendo utilizada para validar e manter a integridade das assinaturas, já a sua chave privada ou secreta, responsabiliza-se pela assinatura dos documentos digitais. Na Figura 3, é demonstrada a geração da assinatura digital.

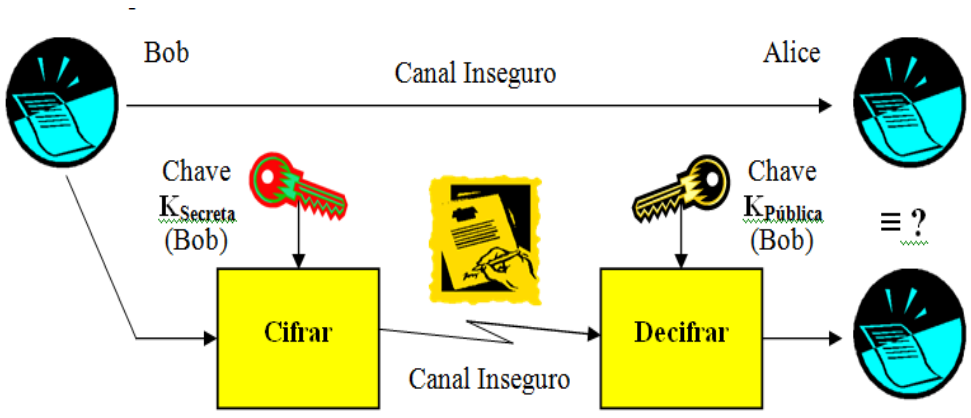

Figura 3 - Geração da Assinatura Digital [GUILHERME 2003].

Nos últimos anos a ICP-Brasil vem produzindo normas e padrões em certificação digital, dentre essas normas temos como destaque o Padrão Brasileiro de Assinatura Digital (PBAD). Essa norma mostra um conjunto de regras que garante a

confiabilidade da assinatura digital, e que podem ser estendidas e verificadas entre todos os sistemas de informação de instituições públicas e privadas [Ramos 2011].

2.2.1 Características da Assinatura Digital

A assinatura digital possibilita garantir a autenticidade, a integridade e não repúdio. Assim, essas características são importantes para a segurança das informações.

Autenticidade

A autenticidade garante a identidade de quem assinou o documento, através da chave privada, única do emissor do documento [Serra 2006].

Integridade

A integridade mostra que se for alterada a mensagem, a assinatura não pertence mais ao documento, ou seja, o documento foi alterado antes de chegar ao seu destino [Pnde 2013].

Não Repúdio ou Irretratabilidade

A irretratabilidade é quando o emissor não pode negar a autenticidade da mensagem. Onde o emissor ao utilizar a chave privada para cifrar o documento, não pode dizer que não foi ele que enviou ou recebeu o documento [ICP-Brasil 2010].

2.3 ICP-BRASIL

A Infraestrutura de Chaves Pública Brasileira – ICP-Brasil constitui um conjunto de práticas, técnicas e procedimentos que fornecem suporte a implementação e a operação de um sistema de certificação digital.

A ICP-Brasil integra uma cadeia hierárquica e de confiança, que garante a autenticidade e a integridade baseada na criptografia de chave pública, assim viabilizando a emissão de certificados digitais para identificação virtual do cidadão [ITI 2011].

2.3.1 Resumo de Mensagem (Hash)

O resumo de mensagem é um método de autenticação que não exige a criptografia de um documento inteiro, ou seja, ele é usado para obter mensagens pequenas e de tamanho fixo. Mais conhecido como função hash, o resumo de mensagem responsabiliza-se por garantir a integridade de um documento digital.

2.3.1 Função Hash

Algoritmos de hash são funções que recebem uma mensagem de tamanho variável e que a transformam em um tamanho fixo. Os algoritmos mais usados são os de 16 bytes (128 bits), que são eles: MD4, MD5 ou o SHA-1 de 20 bytes. O algoritmo MD5 foi produzido em 1991, por Ron Rivest, sendo um algoritmo rápido, simples e seguro. Esse algoritmo foi projetado para suceder o algoritmo MD4, o qual apresentava problemas de segurança. Seu uso se da através de um domínio publico de uso geral e gera um valor hash de 128 bits [ICP-Brasil].

O algoritmo SHA-1 gera um valor hash de 160 bits, a partir de um tamanho arbitrário de mensagem, foi inventado pela *National Security Agency* (NSA), e sua função é a mais usada, pois tem uma grande variedade de aplicações e protocolos de segurança, assim foi considerado o sucessor do algoritmo MD5.

2.4. Certificado Digital

O certificado digital consiste em um conjunto de dados de computador gerado por uma autoridade certificadora, que se destina a registrar, de forma única, exclusiva e intransferível a relação existente entre uma chave de criptografia e uma pessoa física, jurídica ou de máquina [ICP-Brasil 2010].

Essa tecnologia utiliza a técnica de criptografia assimétrica, que possui um par de chaves, uma chave pública e outra privada. Assim, uma pessoa poderá utilizar a chave privada para codificar. Observa-se este procedimento na criação da assinatura digital.

Para que possa ser aceito e utilizado por pessoas, empresas e governos, os certificados digitais necessitam ser emitidos por entidades apropriadas, ou seja, primeiro encontra-se uma Autoridade Certificadora (AC) que tem a função de gerar o certificado digital ou uma Autoridade de Registro (AR).

2.4 Autoridade Certificadora - AC

A responsabilidade por emitir, renovar ou revogar os certificados digitais de outras ACs ou de titulares finais, compete a Autoridade Certificadora, ou seja, esta constitui uma entidade pública ou privada, subordinada à hierarquia da ICP-Brasil. Além disso, cabe à AC emitir listas de certificados revogados [ICP-Brasil 2010].

2.4.1 Autoridade Certificadora Raiz – AC RAIZ

A Autoridade Certificadora Raiz da ICP-Brasil responsabiliza-se por emitir certificados digitais, ou seja, está associada à pares de chaves criptográficas que permitem emitir, expedir, distribuir, revogar e gerenciar os certificados da Autoridade Certificadora [ITI 2010].

O papel da AC-Raiz consiste em executar as políticas de certificados, normas técnicas e operacionais aprovadas pelo Comitê Gestor. A AC-Raiz mostra-se como uma entidade responsável por credenciar, auditar, e fiscalizar as demais entidades da ICP-Brasil [ICP-Brasil 2010].

2.4.1 Autoridade de Registro - AR

Uma entidade de Registro (AR) comprava a identidade do usuário, mantendo uma interface entre um usuário e uma AC, ou seja, ela confere as informações do usuário e emite uma solicitação de certificados a uma AC. A AR tem por responsabilidade a manutenção dos registros de suas operações [ITI 2010].

2.4.2 Padrão X.509

A primeira versão do padrão X.509, recomendado pela *International Telecommunication Union – Telecommunication Stardartization Sector* (ITU-T) surgiu em 1988, sendo conhecida como ITU-T X.509 (V1). Em 1993 surgia a versão V2 e em 2002 foi publicada oficialmente a versão V3.

A especificação X.509 tem como padrão o formato dos certificados digitais, amarrando firmemente um nome a uma chave pública, permitindo autenticação forte. Na ICP-Brasil utilizam-se certificados no padrão X.509 V3 [ICP-Brasil 2010].

2.5. Carimbo de Tempo

O Carimbo de tempo consiste em um documento eletrônico emitido pela Autoridade de Carimbo de Tempo (ACT), que serve para garantir a data e a hora da assinatura digital de documentos eletrônicos em sincronia com a hora legal brasileira (Hora Legal Brasileira – HLB). Regularizado e aprovado pelo Comitê Gestor da ICP-Brasil, o carimbo de tempo garante a validade das assinaturas digitais [ITI 2010].

Carimbo de tempo é uma certidão digital e também uma ferramenta importante para garantir a validade de assinaturas digitais. Com uma referência temporal, o carimbo de tempo, visa atestar a existência de um documento eletrônico em determinado instante de tempo. Para ter validade, a assinatura digital precisa estar ligada a um certificado digital válido, na Figura 4 está especificado o funcionamento do carimbo de tempo na ICP-Brasil [AR CDT 2013].

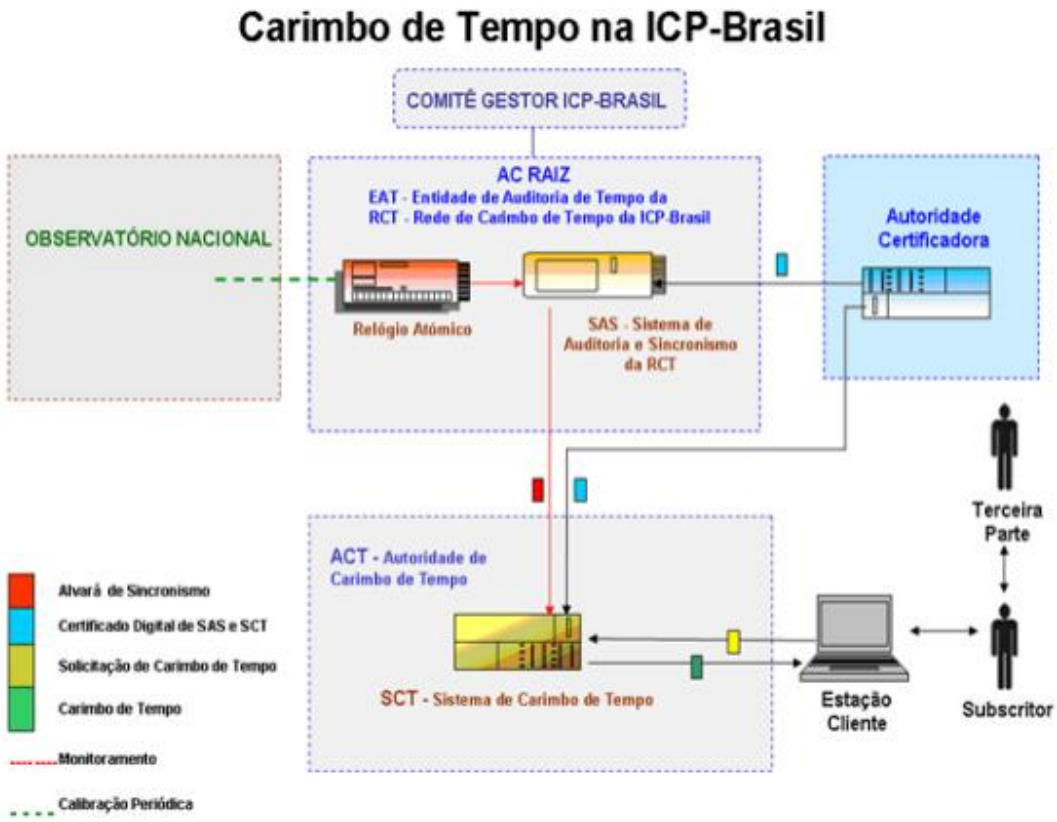

Figura 4 - Modelo de funcionamento do carimbo de tempo da ICP-Brasil [ITI 2010].

3 Trabalhos Relacionados

Nesta seção, são apresentados os trabalhados relacionados, onde o objetivo é avaliar as ferramentas e identificar os desafios encontrados pelos autores.

3.1 Assinatura Digital: Criação de Certificados Digitais para Uso Acadêmico

O trabalho desenvolvido por Lohmann, apresentado junto ao Centro Universitário Franciscano, elaborado como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação do Curso de Sistemas de Informação. Este trabalho tem por

objetivo a criação de certificados digitais do tipo A1, tendo como base o formato ICP-Brasil, para utilização dos mesmos em processos de assinaturas digitais, fazendo com que documentos eletrônicos possam ser assinados digitalmente em ambiente acadêmico [Lohmann 2011].

Lohmann realizou estudos buscando um maior aprimoramento em relação a certificados e assinatura digital, levantando suas funções, características e requisitos necessários para sua utilização. A metodologia de desenvolvimento usada foi o ICONIX e a linguagem de programação C#. O software desenvolvido é capaz de gerar certificados digitais, após obter os dados cadastrais de integrantes desta base de dados ao qual está conectado.

O trabalho apresentou uma possível solução a qual pode ser implementada e utilizada de forma a garantir a integridade e confiabilidade de informações em âmbito interno de uma empresa.

3.2 Segurança da Informação no Ambiente da Internet com Ênfase em Certificação Digital

O trabalho desenvolvido por Bernardinelli, apresentado junto a Faculdade de Tecnologia de Americana, elaborado como exigência curricular do Curso de Processamento de Dados da Fatec de Americana. O objetivo desde trabalho é proporcionar esclarecimentos sobre a certificação digital e ajudar os usuários a obterem um ambiente mais seguro nas redes de computadores, assim reduzindo as perdas de informações, visando uma melhor segurança da informação [Bernardinelli 2010].

O presente trabalho apresentou exigências e cuidados com a certificação digital, que mostra critérios de segurança a serem adotados e implantados para a realização da certificação digital no Brasil, e seus cuidados a serem tomados por quem utiliza a mesma no dia-a-dia.

4 Metodologia

O trabalho foi desenvolvido através de pesquisas bibliográficas sobre o tema Assinatura Digital com ênfase no Carimbo de Tempo. O sistema foi modelado utilizando a metodologia de desenvolvimento de software ICONIX, que consiste em uma metodologia prática e simples, que verifica em todas as fases se os requisitos estão sendo atendidos ou não.

O processo ICONIX trabalha a partir de um protótipo de interface onde se desenvolvem os diagramas, que são divididos em: Modelo de Domínio; Modelo de Caso de Uso; Diagrama de Robustez; Diagrama de Sequencia; Diagrama de Classe. Para fins de compreensão, neste trabalho foram utilizados o Modelo de Caso de Uso e o Diagrama de Classe, onde esses demonstram melhor as funcionalidades do sistema.

A linguagem de programação escolhida foi à linguagem Java, pois ela se mostra uma linguagem rápida, segura e confiável.

4.1 Requisitos

Nesta etapa foi feito o levantamento dos requisitos básicos para o desenvolvimento do software, onde os requisitos são divididos em: Requisitos Funcionais e Não Funcionais. Os Requisitos Funcionais consistem em funções de como o sistema deve reagir e se comportar em determinadas situações. Os Requisitos Não Funcionais consistem em definir as propriedades e as restrições do sistema.

4.1.1 Requisitos Funcionais

- O sistema irá importar um certificado digital;
- O usuário irá informar a senha do certificado digital;
- O usuário poderá assinar esse documento;
- O sistema irá gerar um hash do arquivo;
- O sistema criptografará o hash gerado com a chave privada do usuário;
- O sistema irá gerar um Carimbo de Tempo.

4.1.1 Requisitos Não Funcionais

- Interface Simples;
- O sistema será desenvolvido na linguagem Java.

4.1.2 Modelo de Caso de Uso

O modelo de caso de uso tem por objetivo auxiliar a entre os analistas e o cliente, descrevendo assim um cenário que mostra as funcionalidades do sistema no ponto de vista do usuário. A Figura 5 mostra o modelo de caso de uso, onde o usuário irá fornecer o certificado, a senha e o local do documento que deseja assinar. Ao assinar o documento, o sistema irá gerar um hash do documento, e incluir a assinatura no documento, logo após será gerado o carimbo do tempo no mesmo.

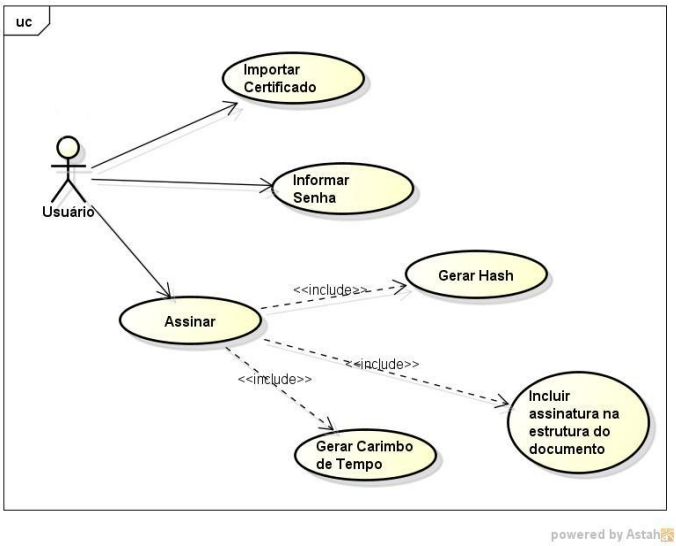

Figura 5 - Diagrama de Caso de Uso.

4.1.3 Diagrama de Classes

O diagrama de classes fornece um conjunto de classes e seus relacionamentos, sua modelagem é orientada a objetos. A Figura 6 mostra o Diagrama de Classes.

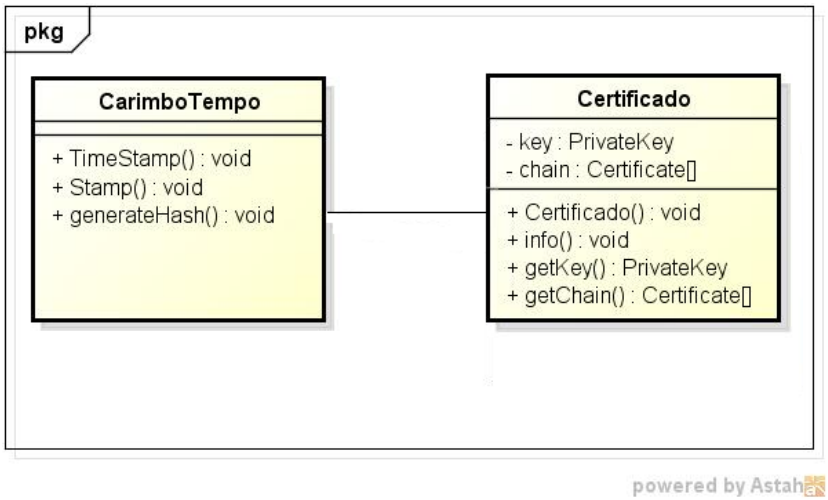

Figura 6 - Diagrama de Classe.

5. Desenvolvimento do Sistema

O protótipo de interface permite testar a funcionalidade e a usabilidade do sistema e assim podendo identificar os requisitos do usuário, assim tendo um maior controle das informações.

A Figura 7 mostra o protótipo de interface que foi criado utilizando a ferramenta NETBEANS IDE. O usuário irá fornecer, através da interface, o local onde o documento e os certificados estão armazenados, bem como a senha do certificado.

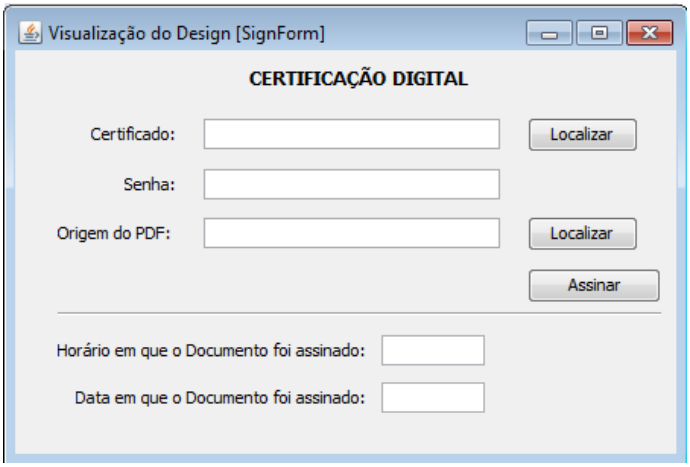

Figura 7 - Protótipo de interface.

O campo CERTIFICADO recebe um certificado do tipo A1, o campo SENHA, recebe a senha própria do certificado, assim o usuário localiza um documento no formato PDF armazenado no seu computador, o mesmo irá assinar o documento clicando no botão ASSINAR, que irá gerar a assinatura e o carimbo do tempo, juntamente com a data e hora em que o documento foi assinado no PDF.

5.1 Assinatura

A assinatura no PDF é um dicionário, um objeto *Dictionary*. Os campos do dicionário possuem informações sobre o signatário. Abaixo estão detalhados os campos utilizados neste trabalho e sua descrição:

- */Contents* – É uma *string* que contém o conteúdo da assinatura codificado em hexadecimal, o PKCS#7[11] da assinatura.
- */ByteRange* – É um array de 4 números. Indica a região de bytes que serão cobertas pela assinatura.

5.2 Certificado

Para extrair as informações necessárias do certificado, foi utilizada a classe KeyStore do Java, que é mostrado nas linhas de código abaixo, onde o *KeyStore* retorna um tipo de armazenamento de chave especifica o *getInstance.*

```
KeyStore ks = KeyStore.getInstance("pkcs12");
Ks.load(new FileInputStream(Cert), password.toCharArray());
String alias = (String) ks.aliases().nextElement();
key = (PrivateKey) ks.getKey(alias, password.toCharArray());
chain = ks.getCertificateChain(alias);
```

5.3 iText

A iText é uma biblioteca que permite criar e manipular documentos PDF. O iText está disponível em Java e C#. Abaixo serão detalhados, de acordo com o iText, as classes utilizadas desta biblioteca no desenvolvimento da aplicação [iText 2011].

- PdfNome
  Deve começar com uma barra seguida de uma sequencia de caracteres ASCII.

- PdfReader
  Possibilita a leitura de um documento PDF. Exemplo:
  ```
  String destino = src.replace(".pdf","[Signed].pdf");
  PdfReader reader = new PdfReader(src);
  FileOutputStream fout = new FileOuputStrem(destino);
  ```

- PdfPKCS7
  Classe que faz todo o processamento ao assinar e verificar um PKCS #7 na assinatura.

- PdfSigGenericPKCS
  Representa um dicionário de assinatura para filtros padrão.

- PdfDictionary
  É uma tabela associativa contendo pares de objetos. O primeiro elemento de cada par é chamado de chave e o segundo é chamado valor. Uma chave pode ser um *PdfName,* enquanto um valor pode ser qualquer tipo de *PdfObject*. Um dicionário é utilizado para coletar e unir os atributos de um objeto complexo, com cada par chave-valor especificando o nome e o valor de um atributo.

6. Resultados

O presente trabalho foi validado através de um arquivo PDF, onde foi submetido à implementação realizada. Após a importação do certificado raiz AC UNIFRA, a assinatura foi validada corretamente através do software Adobe Reader XI.

A Figura 8 apresenta a assinatura e o carimbo do tempo gerado através do Adobe Reader, nesse caso a assinatura foi dada como valida, pois todas as verificações foram satisfeitas. Na Figura 9 temos um painel expandido, onde maiores detalhes da assinatura podem ser visualizados.

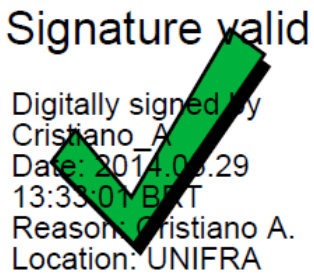

Figura 8 – Carimbo do tempo gerado, com assinatura válida pelo assinante.

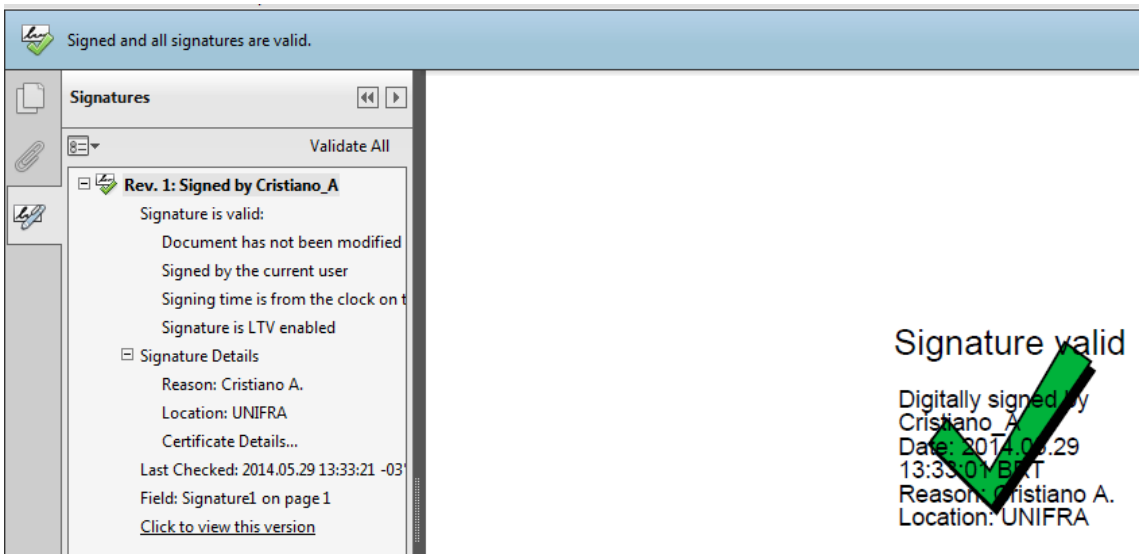

Figura 9 - Documento assinado

Na Figura 10, tem se um exemplo de assinatura desconhecida pelo assinante, isso ocorre quando o certificado da Autoridade Certificadora Raiz Brasileira (ICP-Brasil) não está instalado ou o assinante tenha definido o certificado como de não confiança, assim não o reconhecendo.

Para o assinante tornar seu carimbo do tempo válido ele tem que clicar em cima do carimbo e ir até propriedades da assinatura, assim basta clicar no menu confiança e

adicionar confiança ao certificado e valido-ló. Logo a assinatura se tornará válida para quem o assinou.

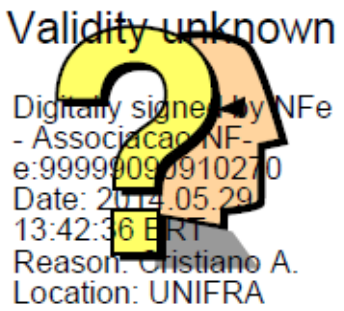

Figura 10 - Carimbo Gerado, com assinatura desconhecida pelo assinante.

7. Conclusão

Nos dias de hoje a assinatura digital vem sendo uma ferramenta importante na proteção dos dados e das informações que trafegam na rede. Assim o presente trabalho passou a estudar a assinatura digital com ênfase no carimbo do tempo.

Estudos foram realizados buscando um maior aprimoramento em relação a certificados, assinatura digital e o carimbo do tempo. Sobre os mesmos foram levantados suas principais características, funções e requisitos necessários para a sua utilização.

A certificação digital é uma tecnologia que visa garantir a segurança da informação, pois documentos assinados digitalmente possuem validade jurídica de próprio punho. Por possuir tal validade, certificados digitais necessitam ser emitidos por entidades apropriadas ou estar de acordo com a política de segurança da empresa.

A implementação deu-se através da metodologia de desenvolvimento de software ICONIX e a linguagem de programação JAVA. Onde a ferramenta mostrou-se simples e eficaz.

Foi analisado que o Carimbo do Tempo certifica a autenticidade temporal de arquivos eletrônicos, juntamente com a data e a hora em que o documento foi assinado.

A referida pesquisa ajudou para um melhor entendimento do desenvolvimento e funcionamento da assinatura digital, a qual ficou comprovada ser um processo seguro e confiável com o auxilio do Carimbo do Tempo.

Em relação à falsificação, não ficou descartada a possibilidade de ocorrer, considerando que as assinaturas digitais acabam perdendo sua validade por enfraquecimentos de algoritmos criptográficos ou pelo comprometimento da chave privada do signatário.

8. Referências

Alecrim, E. Criptografia, infoEster 2009. Disponivel em:

< http://www.infowester.com/criptografia.php>. Acessado em: 22 de Abril 2013.

AR CDT. Autoridade de Registro Centro de Estudos e Distribuição de Títulos e Documentos de São Paulo. Disponível em:<http://www.arcdt.com.br/carimbo_conheca_mais.php>. Acessado dia 06 de junho 2013.

BERNARDINELLI, M. C. R. Segurança da Informação no ambiente da Internet com Ênfase em Certificação. 62p. Monografia (Trabalho Final de Graduação) – Curso de Processamento de Dados, Faculdade de Tecnologia de Americana, Americana. 2010.

Casagrande, A. R. Certificação Digital. 31p. Monografia (Trabalho Final de Graduação) Curso de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Universidade Tecnológica Federal do Paraná, Curitiba, 2011.

Cavalcante, A.L.B. Matemática II. Notas de Aula. Brasília: Editora UPIS (2004).

ICP-BRASIL. Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil: DOC-ICP-01 - versão 4.1. 2010

ICP-BRASIL, Glossário Versão 1.3. 2009. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/Legislacao/Glossario_ICP Brasil_Versao_1.3.pdf>. Acesso em: 15 abr. 2011.

ICP-BRASIL. Estrutura Normativa da ICP-Brasil: Versão 3.6. 2010.

ITI. Instituto Nacional de Tecnologia da Informação. Disponível em: <http://www.iti.gov.br/>. Acesso em: 25 maio. 2013

ITI. O que é Certificação Digital?. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf>. Acesso em: 06 abr. 2011.

Floriano, G. M. CAMOUGLAGED SECURITY SYSTEM: Protótipo de software que emprega técnicas de criptografia, assinatura digital e esteganografia para comunicação segura. 98p. Monografia (Trabalho de Conclusão de Curso), Curso de Sistemas de Informação, Centro Universitário Ritter dos Reis, Porto Alegre, 2007.

Justiça, F. Conselho da Justiça Federal: O que é Assinatura Digital. Disponível em:<http://www.jf.jus.br/cjf/tecnologia-da-informacao/identidade-digital/o-que-e-assinatura-digital>. Acesso em: 10 de maio 2013.

Lohmann, M. Assinatura Digital: Criação de Certificados Digitais para o uso acadêmico. Trabalho de Conclusão de Curso, Curso de Sistemas de Informação, Centro Universitário Franciscano, Santa Maria, 2011.

Mamede, Henrique São. (2006). Segurança Informática nas Organizações. Lisboa/Porto/Coimbra: FCA – Editora de Informática, Ltda

Pnde. Portal Nacional do Documento Eletrônico: Conceito de Assinatura Digital. Disponível em: < http://www.documentoeletronico.com.br/assinatura-digital.asp#1>. Acesso em: 20 de maio de 2013.

Ribeiro, G. Como funciona o Certificado Digital. Disponível em: < http://informatica.hsw.uol.com.br/certificado-digital1.htm>. Acesso em: 05 de maio 2013.

PINHEIRO, Albina. Informática Jurídica. Disponível em: https://www.google.com.br/search?q=PINHEIRO%2C+Albina.+Inform%C3%A1tica+Jur%C3%ADdica.&oq=PINHEIRO%2C+Albina.+Inform%C3%A1tica+Jur%C3%ADdi ca.&aqs=chrome.0.57.239j0&sourceid=chrome&ie=UTF-8>. Acessado em: 10 de junho 2013.

SILVA, Nelson. Preservação por longo prazo de assinaturas digitais. 80p. Dissertação submetida ao Programa de Pós-Graduação. Curso Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2011.

Serra, S. V. Certificação Digital: Uma nova era de segurança eletrônica. 93p. Monografia (Trabalho de Conclusão de Curso). Curso de Sistemas de Informação, Universidade Tiradentes, Aracaju, 2006.