UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Douglas Simões Silva

ESTUDO E IMPLEMENTAÇÃO DO PADRÃO DE REPRESENTAÇÃO VISUAL DE ASSINATURAS PARA PDF

Florianópolis

2014

Douglas Simões Silva

ESTUDO E IMPLEMENTAÇÃO DO PADRÃO DE REPRESENTAÇÃO VISUAL DE ASSINATURAS PARA PDF

Este Trabalho de Conclusão de Curso foi julgado aprovado para a obtenção do Título de "Bacharel em Ciências da Computação", e aprovado em sua forma final pela Ciências da Computação.

Florianópolis, 15 de novembro 2014.

Prof. Vitório Bruno Mazzola
Coordenador do Curso

Banca Examinadora:

Maurício Simões de Oliveira
Universidade Federal de Santa Catarina
Orientador

Prof. Dr. Ricardo Felipe Custódio
Universidade Federal de Santa Catarina
Coorientador

Me. Cristian Thiago Moecke

Sr. Wilson Roberto Hirata

Uma vida não questionada não merece ser vivida.

Platão

RESUMO

Neste trabalho busca se fazer uma revisão bibliográfica sobre assinatura digital e sua representação visual aplicada a *Portable Document Format* (PDF) utilizando a implementação de um software para prova de conceito. O objetivo do estudo é analisar a compatibilidade do padrão de representação visual do *PDF* descrito no documento ETSI TS 102 778-6 (ETSI, 2010) com o padrão brasileiro de assinatura digital. O protótipo desenvolvido, na versão minimalista, tem a intenção de apresentar a representação visual de uma assinatura digital com a adição de uma extensão para logotipos ao certificado.

Palavras-chave: compatibilidade. padrão.

ABSTRACT

This make a literature review on digital signature and the visual representation of that, applied to *Portable Document Format* (PDF) using the prototype implementation such a proof of concept. The aim of this study is to analyze the compatibility of the standard representation visual *PDF* document described in ETSI TS 102778-6 (ETSI, 2010) with Brazilian standard digital signature. The prototype developed in the minimalist version, intends to present the visual representation of a digital signature by adding a logotype extension to the certificate.

Keywords: compatibility. standard.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ETSI	European Telecommunications Standard Institute
ISO	International Organization for Standardization
PDF	Portable Document Format
ICP	Infraestrutura de Chaves Públicas
CMS	Cryptographic Message Syntax
XML	Extensible Markup Language
XMLDsig	XML Digital Signature
PAdES	PDF Advanced Eletronic Signature
CAdES	CMS Advanced Eletronic Signature
XAdES	XML Advanced Eletronic Signature
BER	Basic Encoding Rules
ASN.1	Abstract Syntax Notation 1
AC	Autoridade Certificadora

SUMÁRIO

1 INTRODUÇÃO

Assinaturas digitais são de grande interesse para a comunidade de segurança digital e existem várias formas dessas serem produzidas para documentos eletrônicos. As assinaturas digitais podem ser externas ao documento, anexarem o documento ou serem embarcadas no documento. Para embarcar uma assinatura digital no documento o padrão do documento eletrônico deve prever essa possibilidade. Publicado na norma *International Organization for Standardization* 32000-1 (ISO, 2008), o Formato de Documento Portátil(PDF) idealizado pela Adobe Systems, é um padrão para representação de documentos que possibilita o encapsulamento de assinaturas digitais no próprio arquivo. Em julho de 2010 o *European Telecommunications Standard Institute* (ETSI), organização europeia responsável pela padronização das tecnologias da informação e comunicação, definiu especificações sobre a representação visual de assinaturas digitais para o formato *PDF Advanced Eletronic Signatures* (PAdES).

O *PDF* se mostra um padrão interessante, por ser amplamente utilizado. Como o *PDF* é também um padrão para a visualização de documentos eletrônicos, ele possibilita que a representação visual da assinatura seja anexada ao documento eletrônico. A popularidade desse padrão(Duff Johnson, 2014) pode propagar a utilização da assinatura digital. Isto pode ser observado na imagem(Fig.1)

A possibilidade de ter-se a representação visual de uma assinatura digital dentro de um PDF, tornou pertinente considerar a utilização deste padrão no Brasil. A instituição que normatiza o Padrão Brasileiro de Assinatura Digital(PBAD) é o Instituto Nacional de Tecnologia da Informação(ITI), criado através da medida provisória 2200(Brasil, 2001), essa também que instituiu a ICP-Brasil . Um dos papéis dessa instituição no Brasil é incentivar o uso de tecnologias relativas a segurança digital, entre elas o uso de assinaturas digitais.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

A verificação da compatibilidade do padrão de Assinatura Visual para o formato *PDF* em conformidade com as normas da ICP-Brasil.

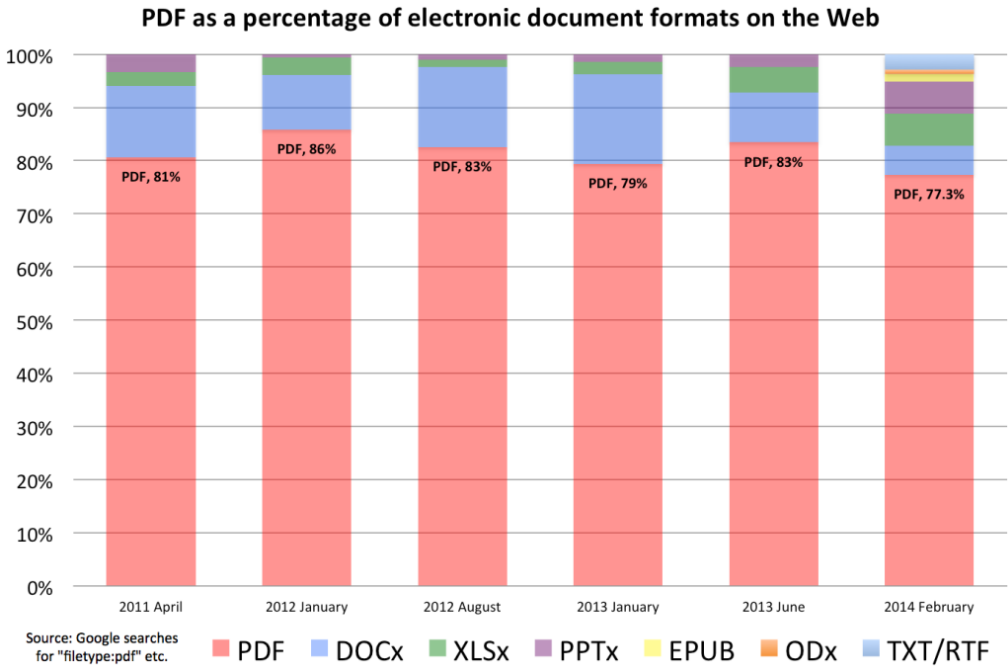

Figura 1 – A porcentagem do *PDF* como formato de representação de documentos na web.

1.1.2 Objetivos Específicos

- verificar a adequação do padrão de representação visual de assinaturas com as normas ICP-Brasil;
- desenvolver uma prova de conceito para o formato *PDF* com a capacidade de produzir uma assinatura visual.

1.2 METODOLOGIA

Neste trabalho foi utilizada a metodologia de comparação de características. O desenvolvimento foi baseado em artigos, padrões e livros referentes ao assunto desta pesquisa. Houve a utilização de uma prova de conceito para validar o trabalho desenvolvido. Foi importante também levar em consideração as normas da ICP-Brasil referentes a

assinatura digital e certificação digital.

1.3 LIMITAÇÕES DO TRABALHO

Como padrão de representação visual de assinaturas exposto pelo ETSI TS 102778-6(ETSI, 2010) explicita os requisitos recomendados, esse trabalho não implementa todas as possibilidades previstas pelo padrão visual. Para que não houvesse sobre carga de conteúdo e fosse aproveitado com maior abrangência as facilidades do padrão, optou-se por escolher uma das recomendações mencionadas no documento. Escolhendo uma aparência da assinatura sem imagem, se estaria abrindo mão do significado e reconhecimento da assinatura pelo usuário, logo foi escolhida a presença de alguma marca ou logotipo. Para que o trabalho abordasse mais tipos de certificados ou seja não apenas aqueles emitidos para pessoas, mas também para empresas e instituições governamentais, não se optou por implementar a assinatura manuscrita (SANTESSON; NYSTROM; POLK, 2004) pois é um perfil restrito a certificados emitidos para pessoas. Portanto, foi adotada nesse trabalho a implementação da extensão de certificados para logotipos, que permite o aproveitamento completo do padrão de assinatura visual para assinatura digital.

1.4 JUSTIFICATIVA

Este trabalho testa a compatibilidade dos mecanismos de aparência da assinatura e representação visual da verificação da assinatura para com as normas da Infraestrutura de Chaves Públicas Brasileira(ICP-Brasil), buscando reduzir a deficiência na usabilidade de segurança(*usable security*) presente na assinatura digital e acrescendo sua escala de utilização.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são descritos os conceitos básicos para o entendimento do trabalho desenvolvido. Esse capítulo é subdividido em Assinatura Digital , Certificado Digital , Infraestrutura de Chaves Públicas e o formato PDF.

2.1 O FORMATO PDF

Segundo a própria Adobe(ADOBE, 2011) o *PDF* teve sua especificação disponibilizada em 1993, mas ainda em formato proprietário até julho de 2008 quando foi oficialmente adotado como padrão aberto pela ISO 32000-1(ISO, 2008). O *PDF* é uma forma digital de representação de documentos. Esse permite aos usuários uma visualização facilitada independente do ambiente onde está foi criada ou visualizada.

2.1.1 Estrutura Fundamental do PDF

De acordo com a ISO32000-1(ISO, 2008) os objetos em um arquivo *PDF* são organizados para otimizar o acesso randômico e ter atualização parcial do arquivo. Um arquivo *PDF* em conformidade com a norma deve ser montado com as seguintes quatro partes, representado na figura 2:

- Um **Cabeçalho** que identifica a versão da especificação do PDF;
- O **Corpo** do documento contendo objetos que descrevem o documento representado pelo arquivo;
- Uma **Tabela de Referência Cruzada** contendo informações sobre os objetos indiretos do arquivo;
- Um ***Trailer*** contendo a localização da tabela de referência cruzada e de alguns objetos especiais dentro do corpo do documento.

2.1.2 Cabeçalho

O cabeçalho do arquivo de *PDF* tem seu significado expresso em uma linha. Esse que identifica qual a versão do *PDF* foi utilizada no

arquivo em questão.

2.1.3 Corpo

O corpo da estrutura do *PDF* é uma sequência de objetos indiretos. Esses representam o conteúdo do arquivo ou os componentes do documento, assim como fontes, páginas e imagens.

2.1.3.1 Objetos Indiretos

Os objetos indiretos são quaisquer objetos que possuam um identificador único para serem posteriormente referenciados. Existem diversos tipos de objetos indiretos como *Boolean*, *Numeric*, *Dictionary*, *Stream Objects*, etc. Os streams de objetos contém sequências de objetos indiretos e sem limite de tamanho, por esta razão objetos com grande quantidade de dados como imagens e vídeos, devem ser representados como streams.

2.1.4 Tabela de Referência Cruzada

A tabela de referência cruzada contém informação que permite o acesso randômico a objetos indiretos. Essa tabela possui uma entrada de uma linha para cada objeto indireto. Inicialmente a tabela consiste em apenas uma seção e conforme a ocorrência da atualização incremental do *PDF* uma seção é adicionada.

2.1.5 Trailer

O trailer possibilita que um leitor *PDF* encontre a tabela de referência cruzada e objetos especiais sem ter de percorrer o arquivo inteiro. Nessa estrutura fica o marcador de final do arquivo.

2.1.6 Atualização Incremental

A atualização do arquivo de *PDF* é chamada de incremental, pois existe o incremento de estruturas no arquivo original. A cada vez que ocorre uma atualização do arquivo são adicionadas as estruturas

Corpo, Tabela de Referência Cruzada e Trailer no arquivo original.

2.1.7 A leitura de um arquivo de *PDF*

A leitura de um arquivo *PDF* é subdividida em duas partes. A primeira parte é a leitura do cabeçalho, logo com essa se tem informação da versão do *PDF* usada no arquivo. A segunda parte seria a leitura do trailer para a localização da tabela de referência cruzada, mas o trailer também pode acessar as tabelas de referência cruzada de outras versões do arquivo até o arquivo original, então a partir do trailer se pode chegar a qualquer versão do arquivo *PDF*.

2.1.8 Assinatura em PDF

De acordo com a ISO 32000-1(ISO, 2008), assinaturas podem ser aplicadas a um documento PDF, sendo referenciadas como *PDF Signature* e devem ser criadas pelo cálculo do resumo criptográfico sobre parte do documento ou todo o documento, sendo o resultado deste cálculo armazenado no próprio documento. As informações da assinatura devem estar contidas no dicionário da assinatura

O *PDF* também inclui características para representar a assinatura eletrônica visualmente, é chamada de aparência da assinatura. A aparência da assinatura é ligada com a assinatura a qual representa. O conteúdo e a aparência da assinatura visual são selados pela assinatura digital convencional.

2.2 *TRANSFORM METHOD*

Antes de se fazer uma atualização incremental no *PDF* é necessário fazer uma análise das modificações do arquivo. Os *Transform Methods* guiam a análise das modificações que ocorrem quando a assinatura é validada. Os valores validos desses métodos são *DocMDP*, *UR*, *FieldMDP*.

2.2.1 *DocMDP*

O *DocMDP* deve ser usado para detectar modificações sobre o campo de assinatura assinado pelo autor. O documento *PDF* pode

conter apenas um campo de assinatura contendo esse método de transformação.

2.2.2 *UR*

O *UR* deve ser utilizado para detectar as mudanças que podem invalidar a assinatura dos direitos de uso do arquivo. A assinatura de direitos de uso é usada para possibilitar a utilização de funcionalidades não disponíveis em um leitor de *PDF* padrão. Essa assinatura deve ser usada para validar as permições que foram concedidas por uma autoridade de concessão de direitos.

2.2.3 *FieldMDP*

O *FieldMDP* deve ser aplicado na detecção de mudanças nos valores de uma lista de formulários. Esse método pode verificar todos os campos de formulário, apenas os selecionados pela entrada *Fields* ou os que não foram selecionados por essa entrada. Essa entrada é apenas um array de texto contendo os nomes dos campos.

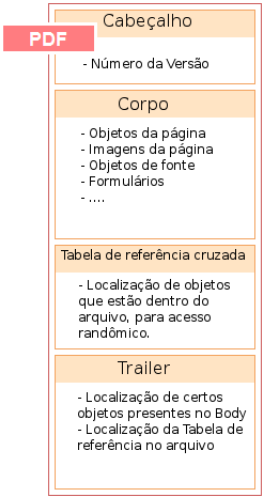

Figura 2 – Estrutura do *PDF*(SIMPO..., 2014).

2.3 ASSINATURA DIGITAL

Segundo o Portal Nacional do Documento Eletrônico (PNDE, 2013), a utilização da Assinatura Digital está cada vez mais comum, com ações, regulamentações do governo e a adoção de seu uso por instituições privadas. A Medida Provisória 2200-2(Brasil, 2001), incentivou a utilização da assinatura digital, pois esta passou a ter mesma validade de uma assinatura de próprio punho.

De acordo com Menezes, Oorschot e Vanstone (MENEZES; OORSCHOT; VANSTONE, 1997), uma grande contribuição provida pela criptografia assimétrica é a assinatura digital. Uma assinatura digital é baseada em uma sequência de bytes obtidos pela aplicação de um algoritmo criptográfico. Segundo Stallings(STALLINGS, 2005) a assinatura digital deve conter algumas propriedades, como verificar o autor, a data e o tempo da assinatura. A assinatura digital serve também deve também autenticar os conteúdos em tempo de assinatura e esta deve ser verificável pelas partes interessadas. Essa serve para proteger a integridade e autenticidade dos dados assinados e garantir o não repúdio do signatário.

2.3.1 Criptografia Simétrica

Segundo Vacca (VACCA, 2009), a criptografia simétrica requer que ambos remetente e receptor tenham a mesma chave secreta, sendo que em cada operação, cifragem ou decifragem, uma chave comum é utilizada. No entanto esse tipo de criptografia tem seus problemas, como o problema de distribuição da chave simétrica entre receptor e remetente, esse problema é resolvido pelo acordo de chaves Diffie-Hellman.

2.3.2 Diffie-Hellman

De acordo com Diffie e Hellman (DIFFIE; HELLMAN, 1976), o custo e o tempo impostos pelo problema distribuição de chaves, eram a maior barreira para a mudança de comunicação de negócios para uma ampla rede de teleprocessamento. Por isto Diffie e Hellman, desenvolveram um protocolo que visa permitir que tanto o receptor e remetente compartilhem suas chaves secretas por meios inseguros de comunicação, para que pudessem se comunicar.

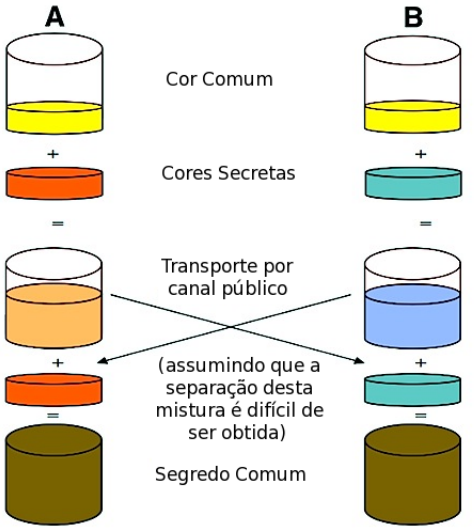

Figura 3 – Ilustração do protocolo Diffie-hellman (VINCK, 2012)

A ilustração 3 exemplifica a solução de Diffie e Hellman utilizando cores. Os dois passos chave deste protocolo é o pré acordo de chave ou cor feito entre A e B por um canal qualquer e a troca de cores secretas ou chaves secretas por uma mistura, que é dificílima de ser revertida. O exemplo termina com A e B possuindo um segredo comum para a troca de mensagens.

2.3.3 Criptografia Assimétrica

De acordo com Paar e Pelzl (PAAR, 2009) , a criptografia assimétrica ou criptografia de chave pública, foi introduzida por Diffie, Hellman (DIFFIE; HELLMAN, 1976). Neste sistema de criptografia há um par de chaves formado por uma chave pública e uma chave privada.

A chave privada deve ser utilizada e conhecida apenas por seu proprietário, a chave pública é de conhecimento público. Pode-se utilizar tanto uma chave pública quanto uma chave privada para cifrar uma informação, desde que se utilize a chave oposta para decifrar a mensagem.

De acordo com Stallings (STALLINGS, 2005), a escolha da chave utilizada na cifragem difere o serviço de segurança obtido pelo emissor nesta operação. Quando a chave utilizada na cifragem é a pública, é obtido o serviço de confidencialidade, assim apenas o receptor da mensagem conseguirá decifrá-la. Quando a chave utilizada é a privada, é obtido o serviço de autenticidade, assim todos que visualizarem esta mensagem comprovarão que o emissor é autentico. Deste serviço de autenticidade é que advém a assinatura.

2.3.4 Assinatura

Segundo Stallings(STALLINGS, 2005), em situações que apenas a autenticação não basta, a solução obtida análoga à assinatura manuscrita, é a assinatura digital. Esta deve possuir as seguintes propriedades para que possa ser equiparada:

- Deve verificar o autor da assinatura;
- Deve autenticar o conteúdo o qual o assinante tem a intensão de assinar;
- Precisa ser verificável por terceiros, resolvendo disputas;

A assinatura pode conter o dado assinado, ou pode estar contida dentro do dado assinado. Para isso deve-se poder assinar apenas partes do documento, que são possibilitadas por três formas de assinatura:

- Assinatura Destacada é a forma de assinar que usa alguma referência para o documento eletrônico assinado para o referenciar como dado assinado.
- Assinatura Embarcada é a mais semelhante com a assinatura manuscrita, pois esta forma de assinar coloca assinatura dentro documento eletrônico assinado.
- Assinatura Envelope é a assinatura que contem o documento eletrônico assinado por ela.

2.3.5 Formatos de Assinatura Digital

Existem vários formatos de assinatura digital e, dentre eles, existem o *Cryptographic Message Syntax* (CMS) e o *Extensible Markup*

Language Digital Signature (XMLDsig). Esses formatos, CMS e XMLDsig, são apresentados nas seções a seguir.

2.3.5.1 *Cryptographic Message Syntax (CMS)*

De acordo com a RFC 5652 (HOUSLEY, 2009) o CMS é um padrão que tem como um dos casos de uso a assinatura digital. O *CMS* define uma sintaxe de encapsulamento para proteção de dados. Essa sintaxe é usada para assinar digitalmente, gerar resumo criptográfico de um conteúdo digital, autenticar ou cifrar determinada mensagem.

Os valores do CMS gerados a partir dos dados encapsulados são gerados usando a sintaxe Abstract Syntax Notation One (ASN.1), codificada em *Basic Encoding Rules*(BER). Atributos assinados e autenticados devem ser codificados em *Distinguished Encoding Rules*(DER) para que assegurem que recipientes possam verificar conteúdos com atributos irreconhecíveis.

2.3.5.2 *Extensible Markup Language Digital Signature (XMLDsig)*

De acordo com Simon, Madsen e Adams (SIMON; MADSEN; ADAMS, 2001), o padrão XMLDsig foi feito para aproveitar as vantagens do XML e da internet. A característica que diferencia o XMLDsig é a capacidade de assinar apenas partes delimitadas do XML, ao invés do documento inteiro. Este padrão pode assinar vários tipos de documentos, como por exemplo, um arquivo de configurações codificado em binário, as classes de um programa e até mesmo uma parte do XML.

2.3.5.3 *XML Advanced Eletronic Signature(XAdES)*

Os padrões XMLDSIG e CMS não tem a característica de assinaturas de longo prazo. O XAdES adiciona as características, geralmente chamadas de propriedades, que são dados extra para explorar determinada finalidade para essa assinatura. Segundo o ETSI TS 101 903(ETSI, 2009) o XAdES especifica perfis para XMLDSIG, provendo a este padrão de assinatura características avançadas e possibilitando aumentar o período em que a assinatura digital permanecerá válida. Os perfis XAdES são *Basic Eletronic Signature*(XAdES-BES), *Explicit policy eletronic signatures*(XAdES-EPES),*Eletronic Signature with Validation Data*(XAdES-T e XAdES-C) e *Archival eletronic signatu-*

res(XAdES-A). O perfil XAdES-BES adiciona propriedades de qualificação ao documento, para este perfil é obrigatória a proteção do certificado do assinante. Segundo o documento do ETSI 101 903(ETSI, 2002), se não for utilizada a propriedade SigningCertificate (que é assinada), deve ser usado o KeyInfo, mas este último deve então ser assinado. O perfil XAdES-EPES extende a definição de uma assinatura eletrônica XAdES-BES apenas incorporando o elemento *SignaturePolicyIdentifier*. O perfil XAdES-T é uma assinatura na qual existe um tempo confiável associado a ela. Este tempo confiável pode ser obtido através de um carimbo de tempo como atributo não assinado adicionado a assinatura ou uma marca de tempo dada por um provedor de serviço seguro. O perfil XAdES-C é uma assinatura com inclusão completa das referências de validação, ou seja adiciona ao perfil XAdES-T as propriedades não assinadas *CompleteCertificateRefs* e *CompleteRevocationRefs*. O elemento *CompleteCertificateRefs* é basicamente uma sequência de referências de um conjunto de certificados de ACs, que é usada para validação da assinatura eletrônica. O elemento *CompleteRevocationRefs* contém uma sequência de referências sobre à revogação dos dados, utilizados na validação do assinante. O perfil XAdES-A é uma assinatura de arquivamento em conformidade com o *CertificateValues* e incorporando o *RevocationValues*, ao invés do elemento *KeyInfo*, que contem respectivamente o conjunto completo de certificados usados para validar uma assinatura eletrônica e com as informações de revogação necessárias para a assinatura.

2.3.5.4 *CMS Advanced Eletronic Signature(CAdES)*

Segundo Pinkas, Pope e Ross(PINKAS; POPE; ROSS, 2008) o formato CAdES pode ser considerado uma extensão para o CMS(HOUSLEY, 2009), adicionando a este, atributos assinados e não assinados, especificando assim perfis para os dados assinados do *CMS*, para sua utilização em assinaturas eletrônicas. O CAdES aborda perfis para as mesmas finalidades que o XAdES, logo existe também perfis CAdES-BES, CAdES-EPES.

2.3.5.5 *PDFAdvanced Eletronic Signature(PAdES)*

De acordo com o ETSI 102 778-2(ETSI, 2009)o PAdES é um formato que tem como característica a possibilidade de gerar assinaturas

equivalentes as especificadas pelos padrões de assinatura CAdES e XAdES. A assinatura PAdES é baseada em CMS assim como o CAdES, sendo que o PAdES tem perfis equivalentes aos do CAdES e XAdES podendo opcionalmente incluir as razões para esta assinatura, a descrição do local em que ela foi feita ou a informação para contato do assinante.

2.4 CERTIFICADO DIGITAL

De acordo com Menezes, Oorshot e Vanstone(MENEZES; OORSCHOT; VANSTONE, 1997), um certificado digital é uma estrutura de dados que consiste de duas partes, uma de dados e uma de assinatura. A parte de dados contém um texto legível, incluindo, no mínimo, a chave pública e um texto identificando a entidade associada a essa chave pública. A parte da assinatura consiste em uma assinatura digital feita por uma Autoridade Certificadora (AC).

2.4.1 Extensões de Certificado

Segundo a RFC 5280(COOPER et al., 2008) extensões de certificado proveem métodos para associar atributos adicionais usuários ou chaves públicas ou Autoridades Certificadoras. Para utilização do padrão de representação visual da assinatura podem ser observadas estas extensões : *Logotypes*, *Biometric Information*, *Certificate Image*.

2.4.1.1 *Biometric Information*

De acordo com a RFC 3739 (SANTESSON; NYSTROM; POLK, 2004) esta é uma extensão opcional para o armazenamento de informação biométrica. Essa informação é armazenada em forma do resumo criptográfico do modelo biométrico. Existem tipos biométricos pré-definidos e na descrição do normativo ETSI TS 102 778-6 (ETSI, 2010), o tipo que deve ser utilizado é o de assinatura manuscrita. Esse tipo quando presente, no certificado de um indivíduo, deve identificar que os dados de origem representam a imagem gráfica da assinatura manuscrita do mesmo.

2.4.1.2 *Logotypes*

Segundo a RFC 3709 (SANTESSON; HOUSLEY; FREEMAN, 2004) e também o ETSI TS 102 778-6 (ETSI, 2010) as pessoas preferem estruturar a informação em categorias e símbolos. A maioria dos humanos preferem fazer a associação entre estruturas complexas com imagens e marcas, pela familiaridade que isto traz a sua memória de reconhecimento(RUGG; YONELINAS, 2003), logo para usuários leigos há uma melhor interpretação e reconhecimento da assinatura digital por meio de um logotipo.

A extensão para logotipos deve referenciar dados de imagens e pode também referenciar dados de áudio. Essas referencias são armazenados no certificado a partir do armazenamento do resultado do resumo criptográfico sobre esses e do caminho que identifica a localização do logotipo na web. A especificação da RFC 3709 (SANTESSON; HOUSLEY; FREEMAN, 2004) categoriza logotipos para representar a organização emissora do certificado, para representar a organização identificada pelo *subject name* do certificado e define uma marca genérica para representar uma comunidade.

Um certificado válido ICP-Brasil, na atual conjuntura, segundo o DOC-ICP-04 versão 5.3 (ITI, 2014) não prevê a referência para imagens no certificado. Para se fazer uma assinatura utilizando o padrão visual de forma completa precisamos de uma imagem certificada ou quaisquer imagem da assinatura manuscrita do dono do certificado e quaisquer imagem de logotipo em questão adicionados ao certificado. Foi utilizada uma extensão adicional chamada *Logotypes* no certificado, que deve se tornar possível para que possa ser utilizada a assinatura visual na ICP-Brasil.

A representação de um logotipo pode ser feita com um ou mais arquivos de imagem. Para que se possa representar um logotipo com uma ou mais imagens, ao menos uma dessas tem que estar na faixa de 60 até 200 pixeis de largura e de 45 até 150 pixeis de altura. Na utilização de varias imagens, essas devem conter variantes semelhantes da mesma imagem. A implementação da representação visual de uma assinatura pode utilizar múltiplos logotipos de diferentes categorias simultaneamente, mas essa não pode mostrar múltiplas variantes da mesma categoria de logotipos. Portanto como exposto pela RFC 3709 (SANTESSON; HOUSLEY; FREEMAN, 2004) cabe a essa implementação assegurar de que não há ambiguidade quanto à ligação entre as imagens e os tipos de logotipos que essas representam.

2.4.1.3 *Certificate Image*

Segundo a RFC 6170 (SANTESSON et al., 2011) que segue o draft mencionado no normativo do ETSI referente ao padrão de representação visual da assinatura, imagem certificada é uma representação visual do certificado definida de acordo com a extensão de logotipos. Para uso dessa extensão define-se uma nova categoria de logotipos chamada *OtherLogos*. Essa extensão deve ser uma representação visual completa do certificado, ou seja a imagem certificada representa todas as informações que o emissor define como relevantes a serem mostradas. O armazenamento dessa acontece da mesma forma que um logotipo.

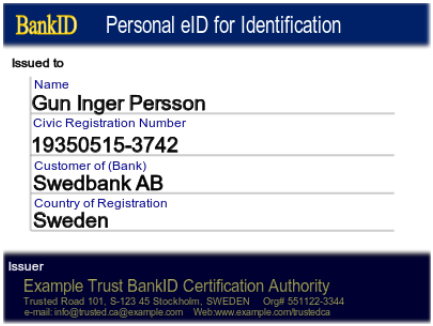

Figura 4 – Exemplo de imagem certificada.

2.5 INFRAESTRUTURA DE CHAVES PÚBLICAS

A estrutura clássica de Infraestrutura de Chaves Públicas (ICP) utilizada no Brasil é a ICP Hierárquica. Ela é chamada de hierárquica pois possui uma hierarquia de Autoridades Certificadoras. De acordo com Housley e Polk (HOUSLEY; POLK, 2001) nessa arquitetura são utilizadas ACs que fornecem serviços para esta ICP, sendo que estas autoridades são relacionadas com a tipo de relação superior-subordinado. As ACs podem ter outras como subordinadas ou podem emitir certificados para usuários finais. Todas ACs possuem uma AC superior com exceção da AC-Raiz.Uma entidade pode verificar o certificado digital de outra montando o caminho de certificação.

2.6 AUTORIDADE CERTIFICADORA

Segundo Housley e Polk (HOUSLEY; POLK, 2001), uma Autoridade Certificadora (AC) é conhecida pelo seu nome e sua chave pública. A AC tem quatro funções principais em uma ICP:

- emitir certificados;
- manter os estados dos certificados(válidos ou revogados);
- publicar certificados válidos e as listas dos certificados revogados(LCRs);
- manter arquivos de informação dos estados sobre os certificados expirados ou revogados que foram emitidos.

2.7 ASSINATURA VISUAL

De acordo com documento*PDF Advanced Electronic Signature Profiles Part 6: Visual Representations of Electronic Signatures* (ETSI, 2010), o padrão de representação visual da assinatura é voltado particularmente para ajudar indivíduos não treinados a entenderem uma assinatura. Deve-se considerar dois aspectos desse padrão a aparência da assinatura e a representação da assinatura quando verificada.

2.7.1 Aparência da Assinatura

Segundo Pope (POPE, 2011), a aparência da assinatura é importante para representação da razão ou intenção do signatário e que o significado da aparência da assinatura deve ser unicamente entendido acompanhado pelo conteúdo do documento. A assinatura pode aparecer tanto abaixo de uma afirmação dizendo que o signatário aceita os termos ou até mesmo abaixo de outras, dizendo que o signatário é testemunha de que o documento foi confirmado pelas partes identificadas como presentes antes dele. A aparência da assinatura é aplicada pelo signatário no momento em que é assinado.

De acordo com o ETSI TS 102778-6(ETSI, 2010), a aparência da assinatura é a representação visual do ato humano de assinar, posto dentro de um documento*PDF* no tempo de assinatura e ligado a uma assinatura digital. A aparência da assinatura tem por objetivo auxiliar o entendimento humano de uma assinatura e oferecer mais consistência

a verificação de uma assinatura eletrônica. Os requisitos recomendados para que se tenha uma aparência de assinatura aplicável a um assinador são:

- Nome do signatário(Commom Name);
- A afiliação do signatário(Organization);
- Quaisquer imagem de logotipo presente no certificado do signatário respeitando a RFC3709(SANTESSON; HOUSLEY; FREEMAN, 2004);
- Quaisquer imagem de uma assinatura manuscrita presente no certificado de acordo com a RFC3709(SANTESSON; HOUSLEY; FREEMAN, 2004);

2.7.2 Representação visual da verificação da assinatura

Segundo Pope (POPE, 2011) a representação visual da verificação da assinatura é importante pois habilita o recipiente do documento para autenticação da identidade afirmada pelo signatário. Este aspecto indica que o documento não foi alterado desde que foi assinado. Essa aplica a autenticação e integridade como um único mecanismo. A representação da verificação da assinatura é aplicada ao recipiente no tempo de leitura do documento quando é necessário ter garantia que a assinatura é autêntica.

De acordo com o ETSI TS 102778-6(ETSI, 2010), quando é verificada uma assinatura a melhor maneira de mostrar as informações resultantes, referentes a validade e integridade, é uma estrutura hierárquica. A representação visual da verificação da assinatura deve no mínimo ter as informações abaixo na sua estrutura hierárquica:

- Validade da assinatura;
- A razão de um resultado inválido ou indeterminado;
- A revisão do documento que a assinatura se aplica;
- O tempo de assinatura e uma indicação do potencial de confiabilidade;
- Informações sobre a identidade certificada;

2.8 ASSINATURA ICP-BRASIL

Segundo o documento DOC-ICP-15 do ITI(ITI, 2010), o uso de assinatura digital com seus respectivos formatos padronizados é imprescindível para que se mantenha a confiabilidade, credibilidade e interoperabilidade da assinatura digital. A assinatura digital deve ser associada por um par de chaves criptográficas, produzida por dispositivo seguro ou não. A assinatura digital deve estar vinculada ao documento eletrônico o qual o assinante teve a intenção de assinar. O par de chaves utilizado na assinatura digital deve ser identificado por um certificado digital ICP-Brasil. Os padrões de assinatura digital aplicam regras de características ou propriedades e determinam políticas de uso dessa.

2.9 POLÍTICA DE ASSINATURA DIGITAL

De acordo com o DOC-ICP-15 do ITI(ITI, 2010) no Brasil foram desenvolvidas dez políticas de assinatura digital, que servem como base para as assinaturas no país. As políticas estão agrupadas por formato, são cinco para o CAdES e cinco para o XAdES. As políticas são correlatos e equivalentes entre um formato e outro com as mesmas propriedades. Essas propriedades justificam os tipos de políticas, segundo o DOC-ICP-15 do ITI(ITI, 2010) são :

- **Política AD-RB**, a assinatura proveniente desta política mais básica é chamada de assinatura digital com referência básica e todos os demais tipos de politicas são incrementados com propriedades a partir dessa.

- **Política AD-RT**, essa política possui a propriedade de referência do tempo, com o atributo não assinado de carimbo de tempo por isso é chamada de política de assinatura digital com referência do tempo.

- **Política AD-RV**, nessa política as propriedades adicionadas são referentes a verificação do momento em que a assinatura é aplicada e com o carimbo do tempo essa permite a extensão do periodo de validade da assinatura e essa política é chamada de política para assinatura digital com referências de validação.

- **Política AD-RC**, os dados necessários para verificação da assinatura são adicionados a assinatura para posterior verificação,

essa política é chamada de política para assinatura digital de referências completas de validação.

- **Política AD-RA**, esse é o tipo de política considerado mais seguro a longo prazo, são retirados alguns dados de referência e um carimbo de arquivamento é adicionado, essa é chamada de política de assinatura digital com referências para arquivamento.

2.9.1 Certificado ICP-Brasil

De acordo com o documento DOC-ICP-04 do ITI(ITI, 2014) na ICP-Brasil todos os certificados emitidos por uma AC responsável devem seguir o perfil x.509 v3 estabelecido pela RFC5280 (COOPER et al., 2008). A ICP-Brasil define também algumas informações do certificado como obrigatórias como as extensões de certificado, identificadores de algoritmo de resumo criptográfico, formatos de nome, restrições de nome e outras informações para se possa considerar um certificado válido. Todas as extensões não previstas no normativo são proibidas e não devem ser utilizadas.

3 DESENVOLVIMENTO

Neste capítulo é apresentada a comparação das características do padrão de representação visual com os requisitos de assinatura digital normatizados pela ICP-Brasil. Para produção da análise foi desenvolvido uma prova de conceito. Este protótipo segue os conceitos descritos na seção(3.1).

3.1 COMPATIBILIDADE ENTRE ASSINATURA VISUAL E ASSINATURA ICP-BRASIL

Os requisitos necessários para uma assinatura visual devem ser satisfeitos também pelas assinaturas digitais ICP-Brasil, mesmo que as informações necessárias para produzir a representação visual não sejam obrigatórias para estas assinaturas.

A representação da verificação da assinatura tem como requisitos recomendados:

- Validade da assinatura, podendo ser representada pelo resultado do verificador;
- A razão de um resultado inválido ou indeterminado, pode ser representada pela verificação detalhada da assinatura;
- A revisão do documento que a assinatura se aplica;
- O tempo de assinatura e uma indicação do potencial de confiabilidade;
- Informações sobre a identidade certificada;

A aparência de uma assinatura PDF(Adobe Acrobat) pode incluir(dependendo da configuração):

- Informação selecionada do certificado digital, que pode ser obtida através das informações do certificado digital, podendo estas estarem inclusas ou serem referenciadas;
- Um gráfico como assinatura manuscrita;
- O tempo da assinatura(usando o relógio local), pode ser representado pelo atributo *id-signingTime*;
- Outra informação posta pelo signatário.

3.2 PROVA DE CONCEITO ORIENTADA A OBJETOS

O software implementado que se utiliza do padrão visual de assinatura digital foi implementado utilizando parte da aplicação desenvolvida para o Padrão Brasileiro de Assinatura Digital(SILVEIRA, 2011). Para que fosse satisfeito o padrão por completo necessitava-se de uma extensão de certificado, que não pertence a nenhum dos perfis previstos pelo DOC-ICP-04 versão 5.3 (ITI, 2014). A fim de que a aplicação conseguisse validar a assinatura foi utilizada uma infraestrutura de chaves públicas de teste. A implementação da prova de conceito seguiu o paradigma da Orientação a Objetos.

3.2.1 Validação da Aparência contra Assinatura Digital

Segundo Pope (POPE, 2011), a assinatura digital, ligada a uma aparência de assinatura, deve ser usada na validação de sua aparência. A autenticidade da aparência pode ser mostrada, pelo leitor de *PDF* arbitrário, na leitura do documento simplesmente baseada na informação da verificação da assinatura digital.

O Adobe Reader mostra a validade da assinatura e informa o motivo desta ser considerada inválida em muitos casos. O leitor de *PDF* deve tentar prover informações em termos simples e não técnicos, para que qualquer usuário consiga entender e esse deve possibilitar a visualização de informações mais detalhadas se necessário.

A informação mostrada na aparência da assinatura esta sob controle da parte de criação do documento. Essa indica apenas a intenção do signatário quando o documento foi assinado, não inferi em nada sobre a integridade, autenticidade ou não repúdio da assinatura digital.

O leitor utilizado não garante que determinada aparência não foi forjada. Por exemplo na imagem(Fig.5) foi referenciada a mesma imagem no certificado(Fig.7) usado para assinar, mas é adicionada outra imagem no dicionário de aparências do *PDF*. No entanto essa alteração não invalida a assinatura em momento algum.

A aparência da assinatura representada como extensão de logotipos no certificado nesse trabalho, de acordo com a RFC 3709 (SANTESSON; HOUSLEY; FREEMAN, 2004) deve ser tratada apenas como uma descrição do emissor. A premissa usada para que a extensão funcione é que os gráficos ou imagens de logotipos, em um certificado, são confiáveis apenas se o caminho de certificação deste certificado é válido. A abordagem de verificação da aparência da assinatura, mencionada na

RFC 3709 (SANTESSON; HOUSLEY; FREEMAN, 2004), é a interpretação humana.

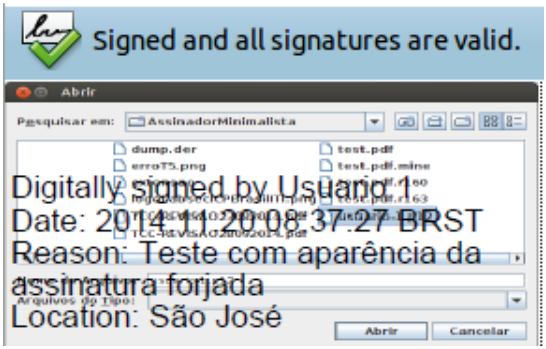

Figura 5 – Assinatura produzida pelo protótipo com aparência forjada.

3.3 PROTÓTIPO

O protótipo visa demonstrar a usabilidade de segurança do padrão de assinatura visual utilizado no Adobe Reader. Para tal foi desenvolvido um protótipo em forma de prova de conceito capaz de realizar assinaturas CAdES seguindo as regras da política AD-RB.

Na implementação do protótipo foi utilizada uma biblioteca, que trabalha com PDF, a iText. Esta biblioteca implementa uma *API* para que seja possível ler,escrever, assinar e verificar a assinatura de um PDF. A iText é compatível com outra biblioteca utilizada na área de segurança digital a *BouncyCastle*.

A aplicação produzida usa um certificado digital e assina um documento. O certificado carregado no protótipo pelo usuário já possui a extensão para logotipos. O documento é assinado de forma destacada, seguindo a recomendação da ISO32000(ISO, 2008) e respeitando as normas da política de assinatura de referência básica(RB). Entretanto antes de gerar a assinatura a aparência da assinatura é adicionada na estrutura do PDF.

A assinatura produzida pelo protótipo pode ser devidamente validada no software de leitura de documentos o Adobe Reader. Os dois conceitos principais do padrão de assinatura visual são mostrados pelo leitor de *PDF*, a aparência da assinatura na posição designada no código da aplicação e a representação da verificação da assinatura quando

o usuário clica na assinatura abrindo o painel de assinaturas.

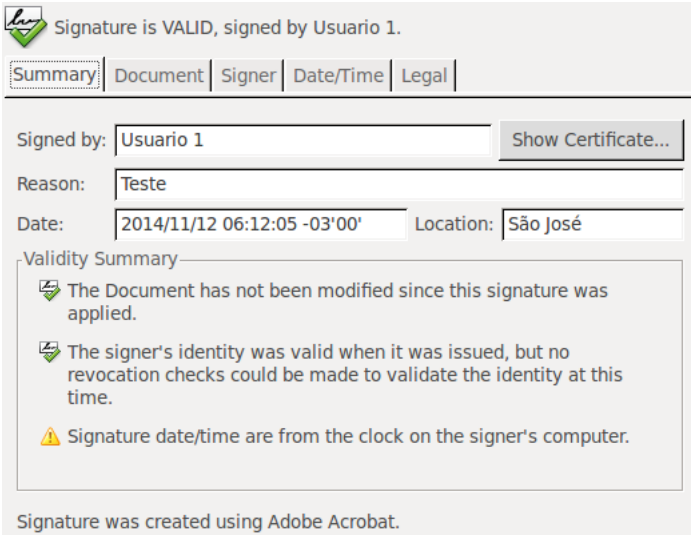

Figura 6 – Representação visual da verificação da assinatura produzida pelo protótipo.

3.3.1 Aparência da assinatura implementada

A aparência da assinatura nessa imagem(Fig.7) esta mostrando o logotipo presente no certificado e mais algumas informações. Foi implementado nesse trabalho o logotipo da categoria *issuerLogo*. Essa categoria segue o mesmo padrão de implementação das categorias de *comunityLogos* e *subjectLogo*, que basicamente podem referenciar o logotipo de modo direto ou indireto.

O modo de referenciamento do logotipo é importante pois em uma futura implementação da verificação de logotipos isto deve mudar como se verifica cada um destes e segundo a RFC 3709 (SANTESSON; HOUSLEY; FREEMAN, 2004) as aplicações devem suportar ambos modos. No modo direto, que foi o utilizado nessa implementação, são colocados no certificado o produto do resumo criptográfico sobre a imagem e uma *URI* que localiza a imagem na web. No modo indireto a *URI* presente na extensão localiza uma *external hashed data structure* que contem informações do tipo, conteúdo e a localização(outras *URIs*)

de cada imagem ou áudio no arquivo. Os dois modos suportam *URIs* alternativas da mesma imagem, para que caso uma imagem não for encontrada seguindo determinada *URI* o usuário tenha outra ou outras localizações para tentar a encontrar.

Sobre a aparência da assinatura existe a representação de informações na forma textual. Essas informações são escolhidas na implementação, na utilização da interface *PdfSignatureAppearance* do iText. A implementação dessa interface permite que sejam alteradas informações como o certificado que aplicará esta aparência, razão do signatário, localização e data que foi assinado o documento em questão.

Figura 7 – Assinatura produzida pelo protótipo.

4 CONCLUSÃO

No desenvolvimento da prova de conceito foram produzidos artefatos relacionados a assinatura digital com o objetivo de incluir a representação visual da assinatura seguindo os padrões da ICP-Brasil. O reconhecimento da assinatura digital que possua alguma imagem para sua representação visual, se mostra consideravelmente melhor, como proposto pelo ETSI, pelo fato do indivíduo que estiver visualizando a imagem gráfica da aparência da assinatura, poder a reconhecer.

Na análise de compatibilidade entre o padrão visual de assinatura digital e as normas da ICP-Brasil concluiu-se que há compatibilidade nas devidas proporções. A representação visual é viável pelas normas da ICP-Brasil apenas na sua forma, sem imagem alguma a ser reconhecida, abrindo mão, em parte, da usabilidade de segurança. Para que haja total compatibilidade o certificado ICP-Brasil válido poderia ter, como opcional, uma extensão para logotipos(SANTESSON; HOUSLEY; FREEMAN, 2004) adicionada a ele, o que na atual conjuntura não é previsto.

O protótipo implementado demonstra que a proposta de representação visual para ICP-Brasil é viável. Entretanto foi observado que as ferramentas utilizadas para validação da aparência da assinatura e da representação visual da verificação da assinatura, necessitam de uma documentação melhor e precisam de uma abordagem melhor que apenas a interpretação humana, para que se possa ter a aparência verificada de maneira automatizada.

4.1 TRABALHOS FUTUROS

Neste trabalho se utiliza um conjunto de tecnologias para chegar ao objetivo de ter uma assinatura digital que utiliza o padrão visual. Este conjunto compreende a prova de conceito, que utiliza o software desenvolvido para o PBAD, em conjunto com a interface do iText para implementação de assinaturas *PDF* em java. A assinatura resultante dessa integração é validada no Adobe Reader.

Como continuação deste trabalho também poderia ser analisada a criação de um plugin referente a assinatura digital. Possibilitaria a aplicação acoplar um assinador que utiliza as normas da ICP-Brasil, podendo este avaliar a conformidade de uma assinatura, que siga o PBAD, com maior precisão.

Outra continuação para esse trabalho seria a validação da aparência da assinatura pelos leitores de *PDF*. Para que essa verificação ocorresse poderia ser implementado um plugin que conferisse se o hash da aparência que esta no dicionário de aparências é igual ao hash da imagem presente na extensão do certificado utilizado. Essa validação poderia ser utilizada tanto para um logotipo quanto para múltiplos.

Poderia ser feita uma análise dos malefícios que o padrão de representação visual da assinatura pode acarretar. Por exemplo se um usuário leigo visualizar a aparência da assinatura e ser induzido a pensar que esta assinatura pertence a outro signatário. A aparência em questão, com as aplicações testadas nesse trabalho, pode ser forjada induzindo a pessoa que recebeu o documento ao erro.

Poderiam ser criadas políticas que determinem as informações mostradas na aparência da assinatura. A partir das políticas de assinatura poderia haver uma verificação sobre os campos mostrados, definindo um formato de texto em que as informações seriam expressas.

REFERENCIAS

ADOBE. *PDF Reference*. 2011. Http://www.adobe.com/devnet/pdf/pdf$_reference.html.Acessoem$: $13nov2014$.

Brasil. *MEDIDA PROVISÓRIA No 2.200-2*. 2001. <www.planalto.gov.br/ccivil$_0$3/$mpv/Antigas_2$001/$2200 - 2.htm$>.

COOPER, D. et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. IETF, maio 2008. RFC 5280 (Proposed Standard). (Request for Comments, 5280). Updated by RFC 6818. <http://www.ietf.org/rfc/rfc5280.txt>.

DIFFIE, W.; HELLMAN, M. New directions in cryptography. *Information Theory, IEEE Transactions on*, v. 22, n. 6, p. 644 – 654, nov 1976.

Duff Johnson. *The 8 most popular document formats on the web*. 2014. <http://duff-johnson.com/2014/02/17/the-8-most-popular-document-formats-on-the-web/>.

ELECTRONIC Signatures a nd Infrastructures (ESI); PDF Advanced Electroni c Signature Profiles ; Part 6: Visual Representati ons of Electronic Signatures. [S.l.], July 2010.

ELECTRONIC Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1. [S.l.], July 2009.

ETSI, T. 101 903-xml advanced electronic signatures (xades). *Signature-Creation Device*, 2002.

HOUSLEY, R. *Cryptographic Message Syntax (CMS)*. IETF, set. 2009. RFC 5652 (INTERNET STANDARD). (Request for Comments, 5652). <http://www.ietf.org/rfc/rfc5652.txt>.

HOUSLEY, R.; POLK, T. *Planning for PKI: best practices guide for deploying public key infrastructure*. [S.l.]: John Wiley & Sons, Inc. New York, NY, USA, 2001. ISBN 0471397024.

ISO. *ISO 32000-1:2008. Document management — Portable document format — Part 1: PDF 1.7*. 2008.

<http://www.iso.org/iso/iso$_c$atalogue/catalogue$_t$c/catalogue$_d$etail.htm?csnumber = 51502>.

ITI, I. N. de Tecnologia da I. *Visão Geral Sobre Assinaturas Digitais na ICP-Brasil. v. 2.0*. apr 2010.

ITI, I. N. de Tecnologia da I. *REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL*. apr 2014.

MENEZES, A.; OORSCHOT, P. V.; VANSTONE, S. *Handbook of applied cryptography*. [S.l.]: CRC, 1997.

PAAR, J. P. C. *Understanding Cryptography*. [S.l.]: Springer-Verlag Berlin Heidelberg, 2009. ISBN 9783642041006.

PINKAS, D.; POPE, N.; ROSS, J. *CMS Advanced Electronic Signatures (CAdES)*. IETF, mar. 2008. RFC 5126 (Informational). (Request for Comments, 5126). <http://www.ietf.org/rfc/rfc5126.txt>.

PNDE. *Portal Nacional do Documento Eletrônico*. 2013. <www.documentoeletronico.com.br/parcerias.asp>.

POPE, N. Visual representation of advanced electronic signatures. In: *ISSE 2010 Securing Electronic Business Processes*. [S.l.]: Springer, 2011. p. 280–290.

RUGG, M. D.; YONELINAS, A. P. Human recognition memory: a cognitive neuroscience perspective. *Trends in cognitive sciences*, Elsevier, v. 7, n. 7, p. 313–319, 2003.

SANTESSON, S. et al. *Internet X.509 Public Key Infrastructure – Certificate Image*. IETF, maio 2011. RFC 6170 (Proposed Standard). (Request for Comments, 6170). <http://www.ietf.org/rfc/rfc6170.txt>.

SANTESSON, S.; HOUSLEY, R.; FREEMAN, T. Internet x. 509 public key infrastructure logotypes in x. 509 certificates. *Internet Engineering Task Force Request for Comments*, n. 3709, 2004.

SANTESSON, S.; NYSTROM, M.; POLK, T. *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*. IETF, mar. 2004. RFC 3739 (Proposed Standard). (Request for Comments, 3739). <http://www.ietf.org/rfc/rfc3739.txt>.

SILVEIRA, L. *Implementação do Padrão Brasileiro de Assinatura Digital*. 2011.

SIMON, E.; MADSEN, P.; ADAMS, C. *An Introduction to XML Digital Signatures*. 2001. <http://www.xml.com/pub/a/2001/08/08/xmldsig.html>.

SIMPO PDF file structure. 2014. <http://www.simpopdf.com/resource/pdf-file-structure.html>.

STALLINGS, W. *Cryptography and Network Security Principles and Practices, Fourth Edition*. [S.l.]: Prentice Hall, 2005. ISBN 0131873164.

VACCA, J. R. *Computer and Information Security Handbook*. [S.l.]: Morgan Kaufmann, 2009. ISBN 9780123743541.

VINCK, A. H. *introduction to public key cryptography*. may 2012. Presentation.

XML Advanced Electronic Signatures (XAdES). [S.l.], June 2009.

ANEXO A – Como utilizar o protótipo

Para realizar uma assinatura utilizando o protótipo deve-se seguir estes passos:

•A seleção do arquivo *PDF* que será assinado;

Figura 8 – Tela inicial do protótipo.

•A seleção do repositório de certificados;

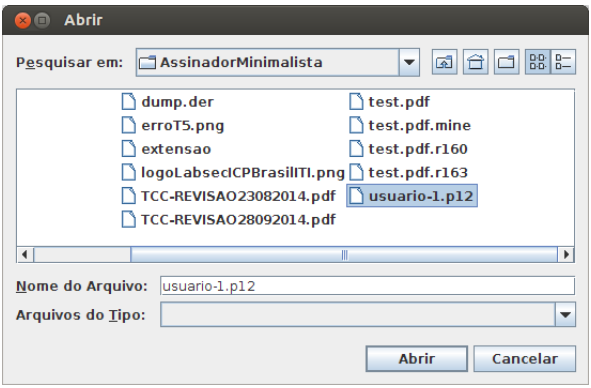

Figura 9 – Escolhendo o repositório.

•Pressione o botão para assinar o arquivo.

•A seleção do alias do qual o certificado utilizado será adicionada a extensão de logotipos.

O arquivo de saída gerado tem nome fixo "teste.pdf"por ser um protótipo para testes.