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

# VERIFICADOR DE CERTIFICADOS E ASSINATURAS ICP-BRASIL EM JAVA

Éttore Leandro Tognoli

Marília, 2012

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

# VERIFICADOR DE CERTIFICADOS E ASSINATURAS ICP-BRASIL EM JAVA

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. Ms. Rodolfo Barros Chiaramonte

Marília, 2012

CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
*BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO*

**TRABALHO DE CONCLUSÃO DE CURSO – AVALIAÇÃO FINAL**

Éttore Leandro Tognoli

VERIFICADOR DE CERTIFICADOS E ASSINATURAS ICP-BRASIL EM JAVA

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

Nota: 9 ( Nove )

Orientador: Rodolfo Barros Chiaramonte

1°. Examinador: César Giacomini Penteado

2°. Examinador: Fábio Dacêncio Pereira

Marília, 04 de dezembro de 2012.

# DEDICATÓRIA

Dedico esta monografia a meu falecido pai.

# AGRADECIMENTOS

A Bárbara, pela paciência e dedicação.

Ao Rodolfo Barros Chiaramonte, pela orientação ,dedicação e as batatas fritas.

Ao Fábio Dacêncio Pereira, pelo incentivo e oportunidades.

Ao César Giacomini Penteado, pelas motivações e por ter sido gentil durante minha defesa.

Ao Fábio(Texugo),Piga, Ivan, Claudinei, Kevin Suellen, Roberta e todos os integrantes da turma de computação, pelos bons tempos passados em conjunto.

Ao Rafael Luiz de  Macedo pelo pudim de todos nós.

Ao Renan, Allan, Rodolfo e a Figurinha pela “água” do paninho.

E a outros mais que ajudaram de alguma forma para a finalização deste trabalho.

# Sumário

# Lista de Figuras

# Lista de Tabelas

## Lista de Siglas

AC – Autoridade Certificadora

ACT – Autoridade de Carimbo de Tempo

ASN1- *Abstract Syntax Notation One*

API – *Application Programming Interfaces*

ICP – Infra-Estrutura de Chaves Públicas

LCR – Lista de Certificados Revogados

OSDT - *Oracle Security Developer Tools*

## Resumo

Para se garantir a autoria de um documento ou contrato é utilizado uma assinatura, para um funcionamento semelhante no meio eletrônico foram concebidas as assinaturas digitais. Este trabalho aborda caraterísticas das assinaturas digitais e demonstra detalhes sobre suas verificações. O objetivo principal é a implementação de um API para a verificação de certificados e assinaturas digitais de acordo com as normas da ICP-Brasil. A ICP-Brasil é o órgão responsável em regulamentar os documentos assinados eletronicamente no Brasil.



Palavras Chave: ICP-Brasil; Bouncy Castle; Certificado Digital; Assinatura Digital; Autoridade Certificadora; Infra-Estrutura de Chaves Públicas



## Abstract

To ensure the authorship of a document or contract is used one signature,to do a similar function on eletronic middle were created the digital signatures. This paper discusses features of digital signatures and give details about their verifications. The main goal is the implementation of an API for verifying digital signatures and certificates in accordance with the standards of ICP-Brazil. The ICP-Brazil is the authority responsible for regulating electronically signed documents in Brazil.



Keywords: ICP-Brasil; Bouncy Castle; Digital Certificate; Digital Signature; Certifying Authority; Public Key Infrastructure

# Introdução

Desde os primórdios o homem registra por meio de escrita, mesmo que rudimentar, a autoria de uma obra ou propriedade, por meio de uma assinatura. A palavra assinatura tem origem no latim "assignare", que significa afirmar, fazer verdadeiro o que está escrito antes. A assinatura está presente nos atos cotidianos como: certidões, contratos, cheques, registros e cartas.

Com o avanço tecnológico a função da assinatura manuscrita foi implementada no meio digital, permitindo a identificação da autoria, coautoria e consenso sobre o conteúdo de um documento digital. Apesar da analogia com a assinatura manuscrita, a assinatura digital é elaborada e validada por sistemas computacionais, utilizando técnicas matemáticas e algoritmos criptográficos. A integração com outras soluções como o certificado digital permitiu não só a garantia de autenticidade, mas também outros serviços como a integridade e o não repúdio sobre um documento digital.

A assinatura eletrônica que é definida por Stallings (2008, p. 272) como “[...] mecanismo de autenticação que permite ao criador de uma mensagem anexar um código que atue como uma assinatura.”; segundo a ICP-Brasil,(2010, p. 4) “[...] esse tipo de assinatura possui o mesmo valor de uma assinatura manuscrita”. Tem, portanto, caráter e valor jurídico. Deve, por conseguinte, ser muito bem definida e documentada afim de que cumpra suas pretensões. Estando no Brasil, existem duas instituições normativas pertinentes: a ETSI e a ICP-Brasil.

Além da implementação da assinatura no meio digital, também existe uma implementação correspondente para os documentos pessoais, estes são o certificados digitais que tem como função principal identificar uma correspondência entre uma assinatura e seu assinante.

Este trabalho terá como produto final um aplicativo que realiza assinaturas digitais com os padrões da ICP-Brasil. O desenvolvimento deste aplicativo foi dividido em módulos, sendo estes o módulo verificador focado neste trabalho e o módulo assinador. O módulo verificador faz verificações em certificados e assinaturas digitais, realizando uma listagem das possíveis anomalias.

## Problemática e Justificativa

Com o grande desenvolvimento da tecnologia e a propagação da internet, foi gerado a necessidade de se realizar transações seguras por meio dela e logo mais a autenticação de documentos eletrônicos. Estas transações e autenticações fazem uso dos conceitos de assinaturas e certificados digitais.

Um certificado digital regulamentado pela ICP-Brasil possui validações diferenciadas em relação aos padrões internacionais; devido a essas diferenças, poucos ou até mesmo nenhum software desenvolvido segue restritamente as devidas validações.

> "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)

## Objetivos

Este projeto tem como objetivo técnico o desenvolvimento de um verificador de assinaturas e certificados digitais, com os padrões estipulados pela ICP-Brasil. Como objetivo cientifico, este trabalho pretende avaliar as normas da ICP-Brasil apontando possíveis melhorias.

### Objetivos Específicos

- Estudo e compreensão das normas da ICP-Brasil
- Implementação das verificações de certificado
- Avaliar as normas referentes a certificados digitais
- Implementação das verificações de assinatura
- Avaliar as normas referentes a assinatura digital

## Trabalhos Correlatos

Há uma grande quantidade de pesquisas e trabalhos relacionados a assinatura e certificados digitais, principalmente dentro da área de direito, estes normalmente questionam sua validade e forma de aplicação. No âmbito de computação a maioria das pesquisas e trabalhos estão relacionados a implementação dos padrões de encapsulamento e sistemas criptográficos.

Para a auxiliar a implementação de aplicativos que envolvem assinaturas e certificados digitais, pode ser feito o uso de algumas APIs, dentre elas podem ser mencionadas a API nativa do Java oferecendo vários recursos para a manipulação de certificados X.509, a API OSDT (*Oracle Security Developer Tools*) que oferece um conjunto de funcionalidades para a geração de assinaturas e a API *Bouncy Castle* utilizada neste trabalho, que possui uma gama de recursos para o desenvolvimento frisado. Porém estas APIs trabalham com certificados e assinaturas de forma genérica sendo necessário a adequação para normas e regulamentações da ICP-Brasil.

Observando as APIs e aplicativos existentes, é notado que os padrões e normas internacionais são mais utilizadas do que as nomas brasileiras, isso se deve ao breve concebimento e a pequena abrangência das mesmas.

## Materiais e Métodos

A proposta inicial foi o  desenvolvimento de um assinador digital completo seguindo os padrões da ICP-Brasil, este projeto foi divido em módulos sendo o foco deste trabalho a pesquisa e implementação das verificações de assinaturas e certificados digitais. O projeto foi apoiado pelo Laboratório de Sistemas Integráveis Tecnológico(LSI-TEC) juntamente ao COMPSI.

Foi realizada uma pesquisa por ferramentas que poderiam acelerar e simplificar o desenvolvimento, esta pesquisa apontou para os seguintes resultados: linguagem de programação Java sendo complementada pela API Bouncy Castle. Os motivos para essas escolhas serão abordados posteriormente no capítulo que descreve as tecnologias utilizadas.

Com a intenção de familiarizar-se com API Bouncy Castle, foram realizadas algumas

implementações utilizando os recursos que seriam necessários no produto final, em seguida foram realizadas especificações e definições do software.

## Organização do Trabalho

Primeiramente o trabalho apresentara os conceitos básicos necessários para a compreensão do contexto começando pela criptografia e suas aplicações, nos capítulos seguintes serão descritos com mais enfase os conceitos utilizados, infra-estrutura de chaves públicas (ICP) , certificados digitais , assinaturas digitais, autoridades certificadoras (AC) e lista de certificados revogados (LCR), posteriormente será apresentado um conjunto de peculiaridades da ICP-Brasil e por fim serão descritos alguns detalhes sobre a implementação do software.

# 1. Criptografia

Criptografia é o estudo de técnicas para transformar informações do seu estado natural compreensível para um estado incompreensível, em outras palavras é utilizado para ocultação do significado da informação.

> "Criptologia: Este é o estudo das técnicas para garantir o sigilo e/ou autenticação da informação. Os dois ramos principais da criptologia são a criptografia, que é o estudo do projeto dessas técnicas; e a criptoanálise, que trata das formas de reverter essas técnicas, recuperar informações ou forjar informações que serão aceitas como autênticas."(Stallings,2008)

No contexto digital a criptografia é utilizada para atender os itens que serão discriminados a seguir.

- Autenticação, é o termo utilizado para verificar se a mensagem em questão foi realmente originada por quem ela diz, garante também que a mensagem não sofreu nenhuma alteração após sua criação.
- Irretratabilidade (Não Repúdio), garante que uma determinada entidade não negue a autoria de sua mensagem.
- Sigilo, alguns tipos de informação tem a necessidade de serem ocultadas para que entidades não autorizadas não possam interpreta-las, assim, o sigilo garante que somente o destinatário verdadeiro possa discernir a mensagem.
- Validade Temporal, tão importante quanto o que foi feito é quando foi feito, para isso é necessário que uma entidade de confiança com um relógio atualizado autentique a mensagem.

## 1.1 Criptografia Simétrica

Um algoritmo de criptografia simétrica faz uso da mesma chave para cifrar e para decifrar a mensagem, sendo assim para que o receptor consiga discernir a mensagem é necessário que ele possua a mesma chave do emissor, ou seja, existe a necessidade do compartilhamento da chave secreta.

Na figura 1 é representado a troca de uma mensagem sigilosa entre duas entidades, a

chave criptográfica é compartilhada entre as duas através de um canal seguro.

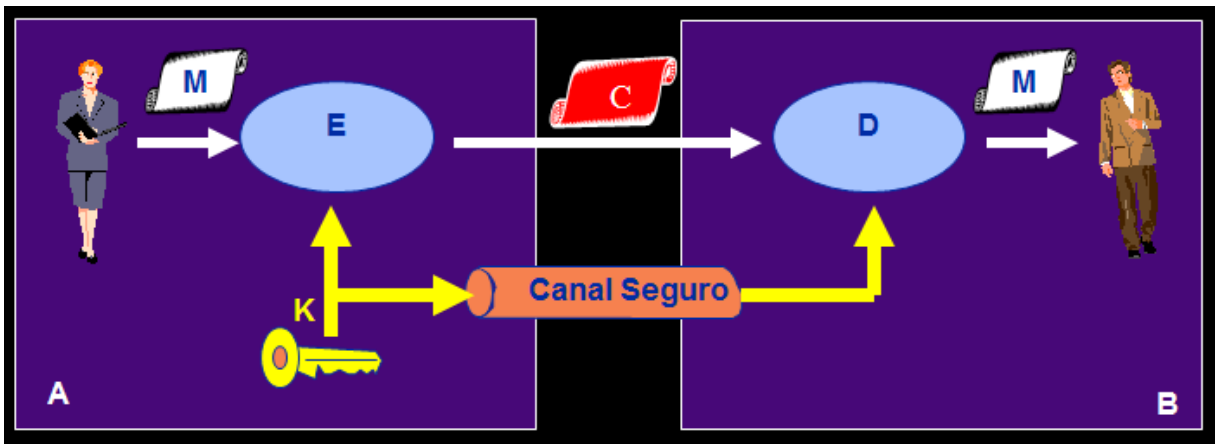


Figura 1 - Processo de cifração/decifração com chave simétrica

Fonte : Guelfi, 2012.

Um exemplo simples de um algoritmo simétrico é a utilização do operador booleano XOR como representado na figura 2; Por exemplo se utilizarmos um byte com o seguinte valor “00100110” como chave e aplicarmos ele no em byte com o valor “10101010” representando uma mensagem, obteremos o seguinte valor “10001100”, isto é então a mensagem cifrada; Aplicando a mesma operação com a mesma chave teremos novamente o valor “10101010”.


Figura 2 -Processo de cifração/decifração com XOR

Fonte : Guelfi, 2012.

## 1.2 Criptografia Assimétrica

Diferentemente dos algoritmos de criptografia simétrica que necessitam que duas ou mais entidades compartilhem a mesma chave secreta, os algoritmos de criptografia assimétrica a mantem em segredo, compartilhando somente uma chave pública, que pode ser distribuída para qualquer um sem ocasionar problemas de segurança. Algoritmos de criptografia assimétrica, fazem o uso de duas chaves complementares, utilizado uma para cifrar e a outra para decifrar, como é representado na figura 3.


Figura 3 - Processo de cifração/decifração com chave assimétrica
Fonte :Guelfi, 2012.

Um exemplo de algoritmo de assimétrico é o RSA, que possui esse nome em função de seus criadores Ronald Rivest, Adi Shamir e Leonard Adleman. A segurança que esse algoritmo proporciona é devido a dificuldade de se fatorar números de grande porte.

## 1.3 Função Resumo (Hash)

A função *hash* é uma função unidirecional que utiliza todos os bits do valor de entrada oferecendo a capacidade de detecção de erros, pois qualquer mudança no valor de entrada altera o resultado da função *hash*.(Stallings,2008). Na figura 4 é demonstrado a aplicação de

uma função *hash*, transformando um elemento de um conjunto M para um outro conjunto H(M). Geralmente o conjunto M possui infinitos elementos e o conjunto H(M) possui uma limitação que depende do algoritmo utilizado.

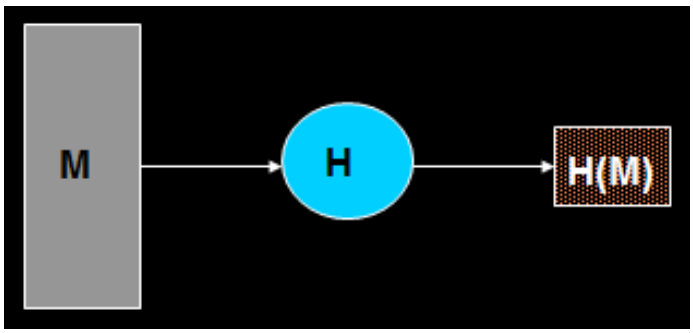


Figura 4- Função de *Hash*
Fonte : Guelfi, 2012.

> "Essas funções são utilizadas para garantir a integridade da mensagem, já que o objetivo delas é gerar um valor y diferente para cada mensagem. Com isso, caso a mensagem x seja modificada para uma x', quando o destinatário receber a mensagem x', terá de recalcular y para a mensagem que recebeu (x'). Como cada mensagem gera um y diferente, ele irá detectar que y para a mensagem que ele recebeu é diferente daquilo que esperava e, com isso, detectar que a mensagem foi alterada." (Moreno;Chiaramonte;Pereira,2005)

## 1.4 Assinatura Digital

Uma assinatura digital tem a função de garantir autenticidade, integridade e irretratabilidade, alguns tipos de assinatura também atendem a validade temporal; para atender todos esses itens a assinatura digital faz uso de uma combinação de recursos criptográficos.

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). Na figura 5 é presentada a troca de uma mensagem assinada entre duas entidades, demonstrando também a forma de verificação.

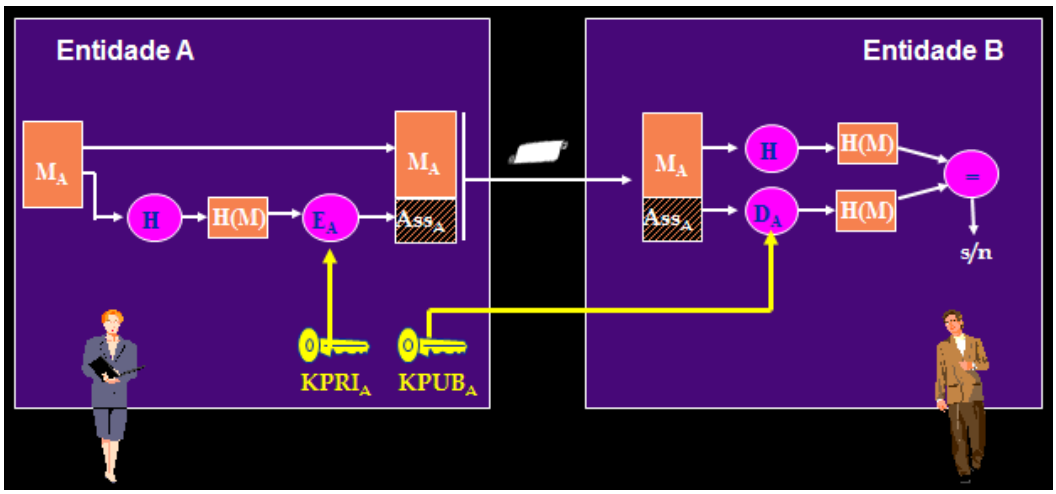


Figura 5- Assinatura digital

Fonte : Guelfi, 2012.

# 2. Infra-Estrutura de Chaves Públicas

Uma Infra-estrutura de Chaves Públicas (ICP), tem como objetivo definir uma estrutura para a emissão de chaves públicas e estabelecer normas e técnicas para a utilização das mesmas, tais normas devem garantir a relação entre uma entidade e seu par de chaves criptográficas e a validade das mesmas.

Para o cumprimento de suas funções uma ICP faz uso de alguns componentes que serão discriminados a seguir, deve-se observar que existem diversas formas de se implementar uma ICP podendo variar a forma de utilização e composição destes componentes.

## 2.1 Certificado Digital

O certificado digital é um item elementar na estrutura das ICPs sendo utilizado na vinculação de uma entidade a sua chave criptográfica, esta vinculação é realizada a partir da assinatura de uma autoridade certificadora. O formato mais comum de certificados é o especificado pela ITU-T chamado X.509, este define a codificação do certificado e as informações neles contidas através do ASN.1. O certificado digital pode ser comparado com um documento de identificação comum (RG;CPF;CNH), mas implementado de forma digital.

## 2.2 Autoridade Certificadora

Uma autoridade certificadora (AC) tem como função básica a emissão de certificados digitais, estes podendo ser destinados a outras ACs ou para usuários finais. Para dar-se início a uma cadeia de certificação é necessário que ao menos uma AC tenham seu certificado auto-assinado, caraterizando-a como uma autoridade certificadora raiz.

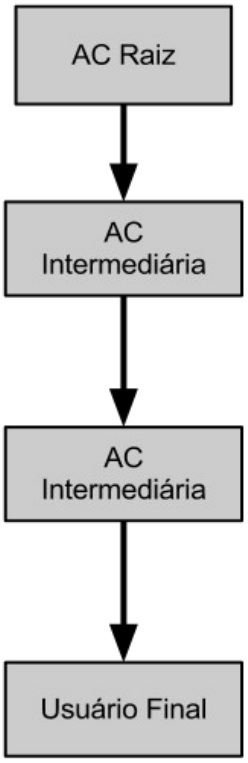


Figura 6- Cadeia de Certificação com Raiz Única

Fonte : Autoria Própria

Algumas ICPs podem possuir mais de uma AC Raiz, neste caso cria-se a necessidade de realizar a certificação cruzada. A Certificação cruzada consiste em que uma AC autentique o certificado de uma outra AC pertencente a uma outra cadeia de certificação, assim criando um elo entre essas duas cadeias. A figura 6 representa uma cadeia de certificação com apenas uma AC Raiz.

Como pode ser observado na figura 6, quando a cadeia possui apenas uma AC Raiz, o fluxo de certificação fica em uma única direção, da AC Raiz até os usuários finais, passando pelas ACs intermediárias. Já em uma cadeia com mais de uma AC Raiz, o fluxo de certificação se torna um pouco diferente, como representado na figura 7.

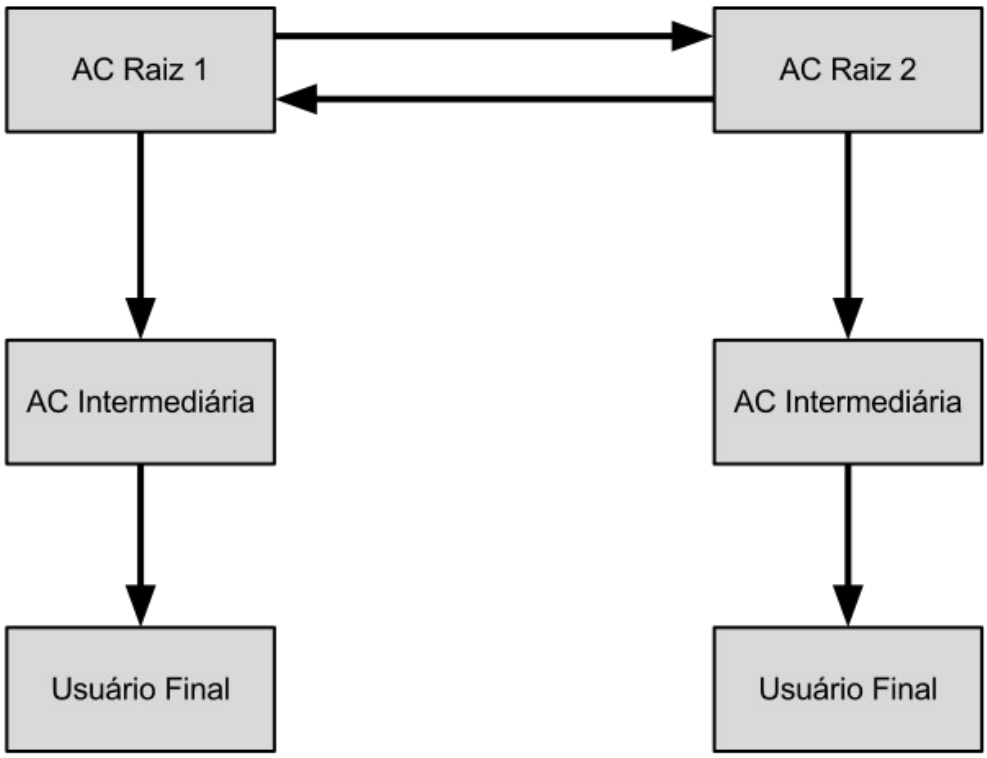


Figura 7- Cadeia de Certificação com Raiz dupla
Fonte : Autoria Própria

## 2.3 Lista de Certificados Revogados

Um Lista de Certificados Revogados (LCR), como o nome já diz, é uma lista de certificados cuja a assinatura não deve ser mais aceita, é muito utilizado nos casos em que o sigilo da chave privada de um certificado e comprometido. Nesta lista além de existir a referência do certificado revogado também existe uma data, esta determina quando a assinatura passou a ser inválida.

Cada AC deve emitir sua própria LCR, esta deve conter somente certificados pertencentes a AC em questão. A LCR deve ser emitida periodicamente, com um intervalo de tempo definido pela normas da ICP utilizada, lembrando que esse intervalo deve ser pequeno para que não exista a chance dos certificados revogados emitirem assinaturas nesta lacuna.

### 2.4 Autoridade de Carimbo de Tempo

Quando se é realizado uma assinatura digital, normalmente é incluído nesta assinatura o horário da maquina local, que não possui um relógio confiável já que o mesmo poderia ser alterado por qualquer um que possuísse as permissões necessárias nesta máquina. Para poder ser incluído um horário confiável na assinatura são utilizadas as Autoridades de Carimbo de Tempo(ACT).

Para uma ACT fazer parte de uma ICP, é preciso que uma AC gere um certificado especifico para ela, este certificado possui características especiais, possibilitando que a ACT realize a emissão de carimbos de tempo.

Um carimbo de tempo é uma assinatura digital realizada por um a ACT, contendo uma referencia de tempo precisa e confiável, normalmente sincronizada com um relógio atômico. O carimbo tem como função afirmar a existência de um documento a partir do momento em que ele é assinado, deve-se observar que isso não significa que a ACT assinante tenha de alguma forma concordado com o conteúdo, mais simplesmente esteja confirmando a existência do mesmo.

## 2.5 CMS

O CMS (*Cryptographic Message Syntax*) é a definição de uma sintaxe para encapsulamento de um documento assinado, um dos padrões de CMS definidos pelo ETSI é demonstrado na figura 8.

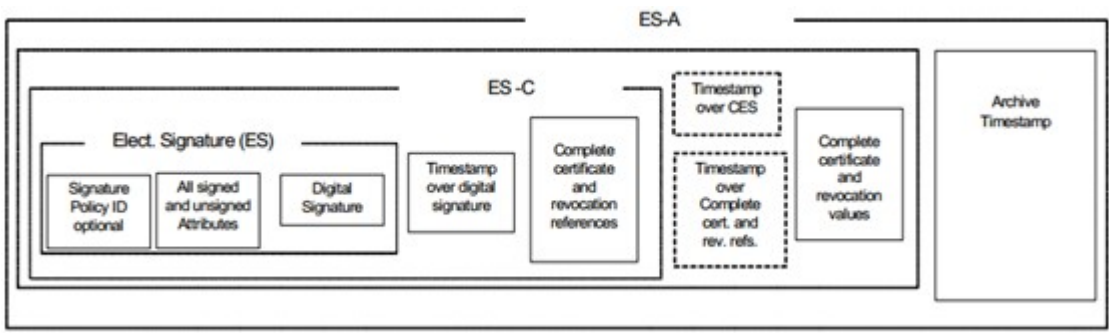


Figura 8- Formato de assinatura ETSI ES-A

Fonte : ETSI, 2003.

# 3. ICP-BRASIL

A ICP-Brasil é ICP responsável em garantir a autenticidade, integridade e a validade jurídica dos documentos eletrônicos no Brasil, sua cadeia de validação está atualmente na versão 3. Esta ICP tem como característica possuir apenas uma AC Raiz, não sendo necessário a realização de certificação cruzada.

> "A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é 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 raíz única, sendo que o ITI 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."(ITI,2012)

## 3.1 Certificados Digitais

Os certificados digitais da ICP-Brasil se baseiam nas especificações ETSI e RFC, estas tiveram algumas modificações julgadas pertinentes pela ICP-Brasil a fim de atender o contexto nacional. A ICP-Brasil faz uso dos certificados não somente com a finalidade de autenticação de servidores ou e-mails, mas também para a autenticação de empresas e pessoas, tendo a necessidade de conter dados que não são de costume de outras ICPs, campos esses como CPF e CNPJ.

## 3.2 CMS

Os padrões de CMS da ICP-Brasil também foram baseados em especificações internacionais, mas também como os certificados sofreram algumas alterações. Uma das alterações foi, criar políticas diferenciadas para cada tipo de assinatura, sendo que essas políticas devem ser assinadas. Esta modificação causa uma grande dificuldade em realizar transições de tipos de assinatura, este assunto será mais abordado posteriormente.

A figura 9 representa o padrão AD-RA, que é o padrão mais completo, este engloba as características dos demais padrões como representado na figura.

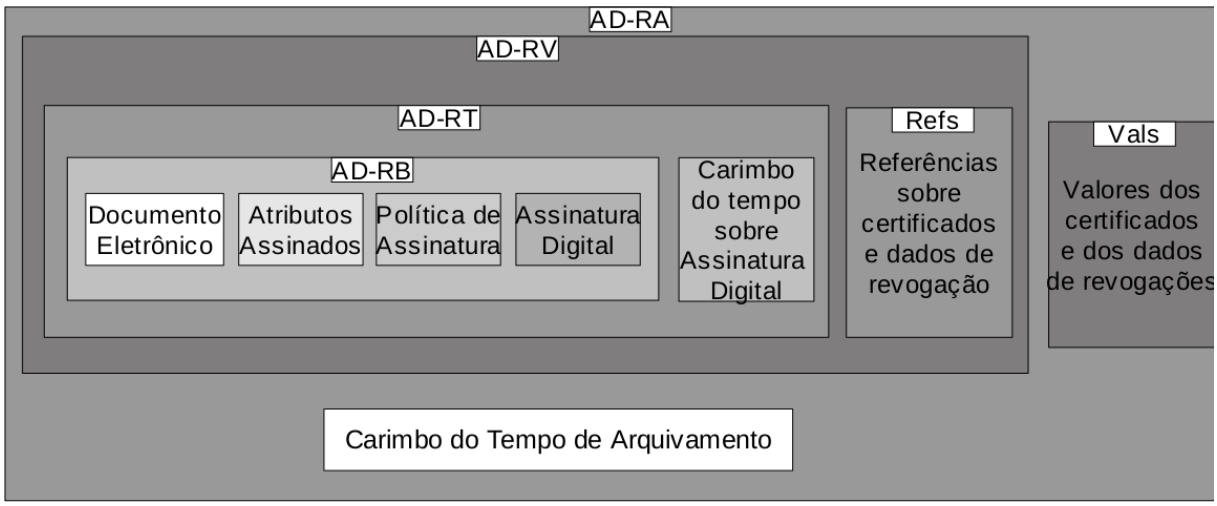


Figura 9 - Formato de assinatura AD-RA

Fonte : ICP-Brasil 15.01, 2010.

### 3.3 Autoridade Certificadora Raiz

A ICP-Brasil possui atualmente quatro cadeias de certificação, cada uma possuindo um AC Raiz independente, sendo elas : Autoridade Certificadora Raiz Brasileira; Autoridade Certificadora Raiz Brasileira v1 ; Autoridade Certificadora Raiz Brasileira v2 ; Autoridade Certificadora Raiz Brasileira v3. Suas principais diferenças são a data de expiração, e os algoritmos criptográficos utilizados, sendo que a primeira versão (Autoridade Certificadora Raiz Brasileira) encontra-se expirada desde 31/11/2001, e a ultima versão (Autoridade Certificadora Riz Brasileira v3) expira-rá em 21/06/2023.

> "A Autoridade Certificadora Raiz da ICP-Brasil é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC- Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subseqüente ao seu."(ITI,2012)

> "A AC-Raiz também está encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as Autoridades Certificadoras – ACs estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor. "(ITI,2012)

### 3.4 Autoridade Certificadora

A maioria das autoridades certificadoras da ICP-Brasil, pertencem a entidades de confiança como o SERASA, CASA DA MOEDA e outras mais. A utilização de ACs auxiliam da divisão de responsabilidades, desta forma cada AC fica responsável por alguma determinada área de atuação.

> "Uma Autoridade Certificadora é uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Desempenha como função essencial 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 (pública/privada). "(ITI,2012)

### 3.5 Autoridade de Registro

Para que os certificados regulamentados pela ICP-Brasil sejam de confiança é fundamental que não existam fraudes na emissão dos mesmos, é responsabilidade da autoridade de registro (AR) validar todos os documentos necessários para emissão do certificado.

> "Entidade responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC que tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota ." (ITI,2012)

### 3.6 Autoridade de Carimbo de Tempo

As ACT ainda são um assunto um tanto quanto recente para o Brasil, atualmente não existe nenhuma ACT homologada pela ICP-Brasil, era previsto que em 2011 alguma já estivesse em funcionamento.

“Ao assinar um documento eletrônico, é preciso ter certeza da hora em que a transação foi feita. Atualmente, a data é dada pelo relógio do próprio computador do usuário que nem sempre é correta. Assim, o carimbo de tempo ou datação eletrônica é do que uma forma segura de agregar e registrar a hora em que determinado certificado concluiu uma operação eletrônica”(ITI,2012)

# 4. Validações

A seguir serão descritos os procedimentos para a validação dos certificados e assinaturas, de modo a discriminar as validações genéricas de uma ICP e as especificadas pela ICP-Brasil.

## 4.1 Certificado Digital

A validação de um certificado digital basicamente depende do certificado de sua AC, que contem a chave pública necessária para decifrar a assinatura contida no certificado a ser verificado, então primeiramente deve ser obtido os dados identificadores da AC, para que assim ela possa ser localizada e requerida.

A estrutura de um certificado digital possui alguns campos para auxiliar na obtenção e identificação de sua CA, como seu nome, uma ou mais URLs para realizar o *download* da cadeia de certificação, o identificador da chave pública. Os tipos destes campos dentro do certificado podem variar de acordo suas respectivas versões.

Após a verificação criptográfica do certificado é necessário verificar se o mesmo está revogado. Para isso é imprescindível possuir a LCR mais atual emitida por sua AC. A LCR também é um documento assinado e deve ser validado como todos. Caso o certificado esteja na lista de certificados revogados o mesmo não deve ser mais considerado válido a partir do momento de sua revogação.

Finalizado o processo de validação do certificado em questão, é necessário realizar os mesmos procedimentos para todas as ACs de sua cadeia, com um foco especial nos valores que somente ACs possuem, uma AC deve possuir alguns *bits* de ativação dentro do certificado, estes que definem se o certificado em questão pode ser utilizado para emitir outros certificados.

## 4.2 Certificado ICP-Brasil

Um certificado ICP-Brasil, além de abranger todas as validações de um certificado comum, contem algumas restrições de codificação, políticas e conteúdo.

As políticas da ICP-Brasil classificam o certificado pelo seu grau de segurança e pelos tipos de utilização, a tabela 1 demonstra algumas características de segurança dos certificados com propósito de assinatura.

Tabela 1- Detalhes dos certificados

| | A1 | A2 | A3 | A4 |
|---|---|---|---|---|
| **OID Politica** | 2.16.76.1.2.1.N | 2.16.76.1.2.2.N | 2.16.76.1.2.3.N | 2.16.76.1.2.4.N |
| **Algoritmo de HASH** | SHA1 ou SHA256 | SHA1 ou SHA256 | SHA1 ou SHA256 | SHA1 ou SHA512 |
| **Algoritmo de Criptografia** | RSA | RSA | RSA | RSA |
| **Tamanho da Chave** | 1024 ou 2048 bits | 1024 ou 2048 bits | 1024 ou 2048 bits | 2048 ou 4096 bits |
| **Duração** | 1 Ano | 2 Anos | 3 Anos | 3 Anos |
| **Armazenamento da Chave** | Arquivo | Arquivo | SmartCard \| Token | SmartCard \| Token |

Para determinar o propósito do certificado é necessário uma análise do valor do campo "*KeyUsage*", na tabela 2 é demonstrado os valores do campo "*KeyUsage*" para os certificados da ICP-Brasil, sendo A certificados com propósito de assinatura, S certificados com propósito de sigilo, T certificados de ACT e AC para certificados de autoridades certificadoras.

Tabela 2- Detalhes do *KeyUsage*

| | A | S | T | CA |
|---|---|---|---|---|
| **digitalSignature** | 1 | 0 | 1 | 0 |
| **nonRepudiation** | 1 | 0 | 1 | 0 |
| **keyEncipherment** | 1 | 1 | 0 | 0 |
| **dataEncipherment** | 0 | 1 | 0 | 0 |
| **keyAgreement** | 0 | 0 | 0 | 0 |
| **keyCertSign** | 0 | 0 | 0 | 1 |
| **cRLSign** | 0 | 0 | 0 | 1 |
| **encipherOnly** | 0 | 0 | 0 | 0 |
| **decipherOnly** | 0 | 0 | 0 | 0 |

Além das restrições do "*KeyUsage*" os certificados também são diferenciados através do "*BasicConstraints*" e do "*ExtendedKeyUsage*". O "*BasicConstraints*" é utilizado

basicamente para definir se é um certificado de usuário final ou de uma AC, no caso da AC ainda pode definir o nível hierárquico do certificado, apesar de isso ser pouco utilizado dentro das cadeias da ICP-Brasil. O "*ExtendedKeyUsage*" é um extensão do "*KeyUsage*" definindo outras utilidades do certificado. Na tabela 3 é representado os valores de "*ExtendedKeyUsage*" para certificados de usuários finais para o fim de assinatura (A1-A4) e de certificados de ACTs (T3 – T4).

Tabela 3-Detalhes *Extended Key Usage*

| | **A1 – A4** | **T3 – T4** |
|---|---|---|
| **id_kp_clientAuth** | 1 | 0 |
| **id_kp_emailProtection** | 1 | 0 |
| **id_kp_timeStamping** | 0 | 1 |

No padrão X.509 existe o "*SubjectAlternativeOtherName*", este responsável em armazenar nomes complementares para o dono do certificado, para a ICP-Brasil, é utilizado para armazenar alguns valores obrigatórios, no caso documentos pessoais que variam entre pessoa física e pessoa jurídica. Através do "*SubjectAlternativeOtherName*", deve ser identificado se o certificado pertence a uma pessoa jurídica ou a uma física, para que assim possa ser verificado se o mesmo possui todos os campos obrigatórios.

## 4.3 CMS

A validação de um CMS depende inteiramente de conter o certificado do assinante, para isso o CMS, contem campos para auxiliar na identificação de seu assinante, estes campos podem variar de acordo com a versão.

Nas versões mais antigas de CMS eram utilizados como identificador do assinante, o nome da AC e o numero de série do certificado do assinante, nas versões mais atuais é utilizado o "*PublickeyIdentifier*" que é um *hash* da chave pública do assinante.

Como o CMS é um forma de encapsulamento de assinaturas, ele permite a inserção de varias assinaturas no mesmo arquivo, cada assinatura é contida no "*SignerInfo*", este possui as informações necessárias sobre o assinante e a assinatura para que estes possam ser validados. Nos padrões ETSI, é possível que cada "*SignerInfo*" tenha um padrão diferenciado, por

exemplo, em um mesmo CMS , seria possível ter uma assinatura comum e mais outra com um carimbo de tempo.

### 4.4 CMS ICPBrasil

O tipo mais básico de assinatura da ICP-Brasil é o AD-RB, este tem como finalidade a autenticação e irretratabilidade de um documento. O documento assinado pode ou não estar contido dentro da assinatura, caracterizando a assinatura como "*attached*" ( contendo o arquivo) ou "*detached*" (apenas a referencia do arquivo) .A figura 10 representa a estrutura de uma assinatura AD-RB.

Para a validação do AD-RB é necessário realizar as verificações criptográficas padrões, ou seja, decifrar a assinatura e compará-la com o *hash* do documento assinado, deve também ser verificado a política, que deve ser umas das quatro possíveis dentro de um AD-RB, sendo elas: AD-RB 1v ; AD-RB 1.1v ; AD-RB 2v ; AD-RB 2.1v. Deve também ser verificado se outras assinaturas dentro do CMS seguem os padrões de um AD-RB.


Figura 10 - AD-RB
DOC-ICP-15.01, 2008.

O padrão AD-RT é quase como uma extensão do AD-RB como representado na figura 11. Este vem com adição de um carimbo de tempo para garantir a validade temporal da assinatura, suas validações incluem as pertinentes a do padrão AD-RB. Devido ao carimbo de tempo, é necessário realizar algumas validações extras. Deve ser validado o próprio carimbo de tempo, e ser comparado a data do carimbo com data de assinatura do CMS, a data de assinatura deve ser anterior a data do carimbo.

No caso do certificado do assinante se encontrar revogado deve ser observado a data de revogação e compara-la com a data do carimbo, a data de revogação deve ser posterior a do carimbo, isso garante que assinatura foi realizada antes do certificado ter sido revogado.

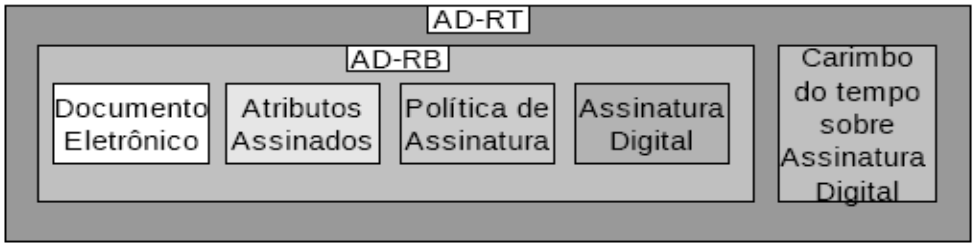


Figura 11 - AD-RT

Fonte : DOC-ICP-15.01, 2008.

O padrão AD-RV encapsula o AD-RT, tendo como adicional referencias para a validação do CMS, estes adicionais contem o *hash* dos certificados e das LCRs utilizadas para a verificação no momento da assinatura, esta referencia ainda é carimbada, ver figura 12. Estes adicionais devem ser validados no momento da leitura do CMS, juntamente com as outras validações dos padrões encapsulados.

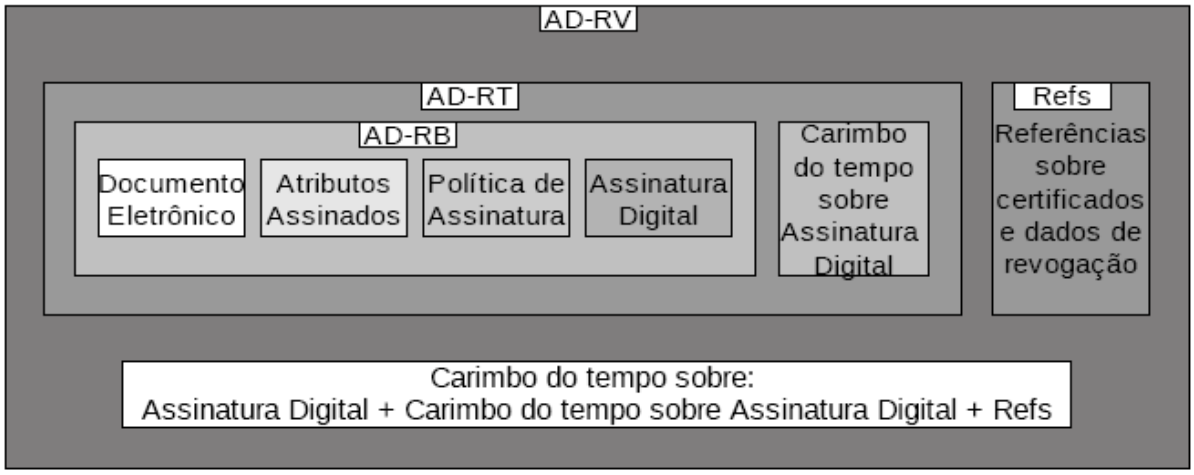


Figura 12-AD-RV

Fonte : DOC-ICP-15.01, 2008.

O padrão AD-RC encapsula o padrão AD-RV, e adiciona os certificados e LCR utilizadas na verificação da assinatura e na geração das referencias do AD-RV, como mostrado na figura 13.

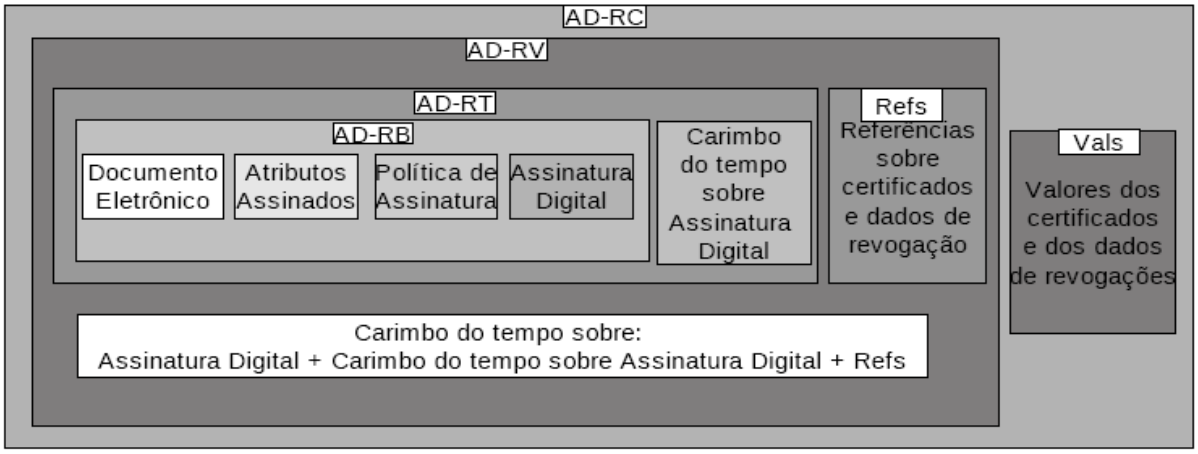


Figura 13 - AD-RC
Fonte: DOC-ICP-15.01, 2008.

O ultimo e mais complexo padrão é o AD-RA este é utilizado para o armazenamento de assinaturas. Como com o passar do tempo os algoritmos de criptografia vão se tornando obsoletos e inseguros, as assinaturas antigas necessitam de um reforço criptográfico, para isso devem ser utilizados recursos criptográficos mais atuais. O reforço criptográfico é realizado através de um carimbo de tempo de arquivamento, como demonstrado na figura 14.

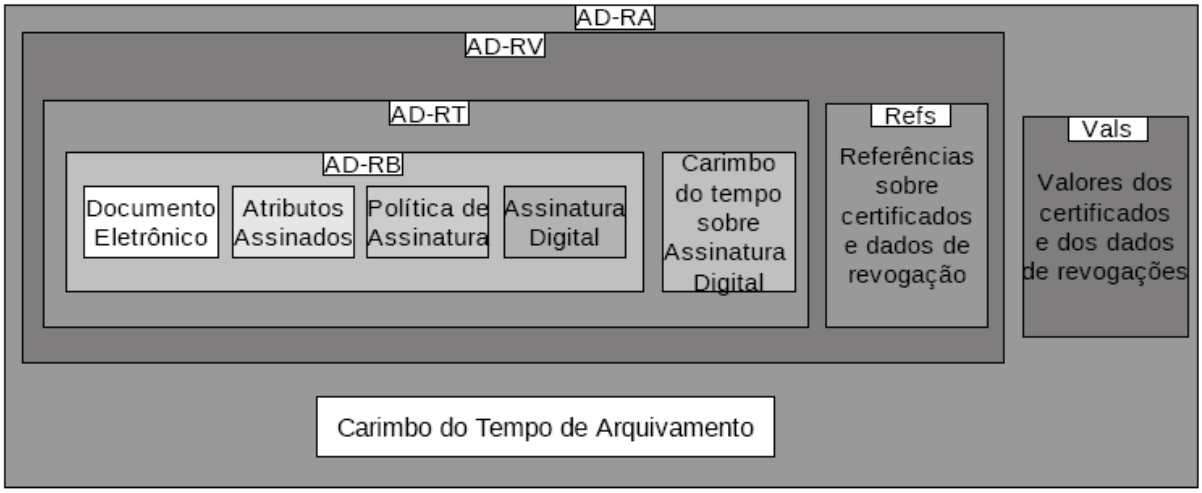


Figura 14 - AD-RA
Fonte: DOC-ICP-15.01, 2008.

# 5. API de verificação ICP-Brasil

Este capitulo abordará as tecnologias utilizadas e características técnicas do desenvolvimento.

## 5.1 Tecnologias

Para a implementação final do verificador de certificados e assinaturas digitais, foi utilizado um conjunto bem especifico de tecnologias, estas serão descritas a seguir.

Java /JCE: Java é uma linguagem de programação orientada a objeto independente de plataforma, possui uma API nativa com muitas funcionalidades, abrangendo também a área de segurança dando suporte nativo a certificados X.509. A aplicação desenvolvida foi puramente escrita em Java (versão 7).

Bouncy Castle: A API Bouncy Castle veio a complementar os recursos nativos do Java, além de possuir classes que auxiliam no manuseio dos certificados, oferece também algoritmos criptográficos e suporte a documentos assinados. Está API foi muito utilizada para extração dos dados dos certificados e assinaturas, tornando possível as validações necessárias.

Smart Card: Alguns tipos de certificados da ICP-Brasil tem como definição que a chave privada seja armazenada em um cartão inteligente(*Smart Card*) ou em um *token*. Para que fosse possível integrar esses tipos de certificados ao aplicativo foi necessário utilizar alguns *drivers* para comunicação com os *Smart Cards*. A empresa LSI-TEC forneceu alguns *Smart Cards* com certificados para testes, estes possuem *drivers* somente para o Windows, dificultando os testes em outros sistemas operacionais.

SQLite: O SQLite é uma biblioteca desenvolvida em linguagem C padrão ANSI, oferece suporte a diversas linguagens de programação, dentre elas JAVA; É um software livre, evitando preocupações com licenças de uso, é multiplataforma e não necessita de instalação ou de um servidor, essas e outras características tornaram o SQLite perfeito para aplicação desenvolvida.

Sign Server: O SignServer é uma estrutura de aplicativo para executar operações criptográficas para outras aplicações. É destinado a ser utilizado em ambientes onde as chaves deveriam estar protegidos em hardware, mas não é possível.(SIGNE SERVER, 2012)

## 5.2 Estrutura

O aplicativo assinador como dito anteriormente foi dividido em módulos, sendo eles módulo de assinatura e  módulo de verificação de certificados e assinaturas. A figura 15 demonstra sucintamente a forma como os módulos serão utilizados na aplicação completa. O módulo de verificação encontra-se destacado por ser o foco deste trabalho. O módulo de assinatura faz uso do módulo de verificação para que possa obter a chave privada do assinante, esta deve estar instalada na *key store* do sistema operacional. O módulo de assinatura também utiliza o módulo de verificação para obter documentos uteis a geração da assinatura, como o certificado e a lista de certificados revogados.

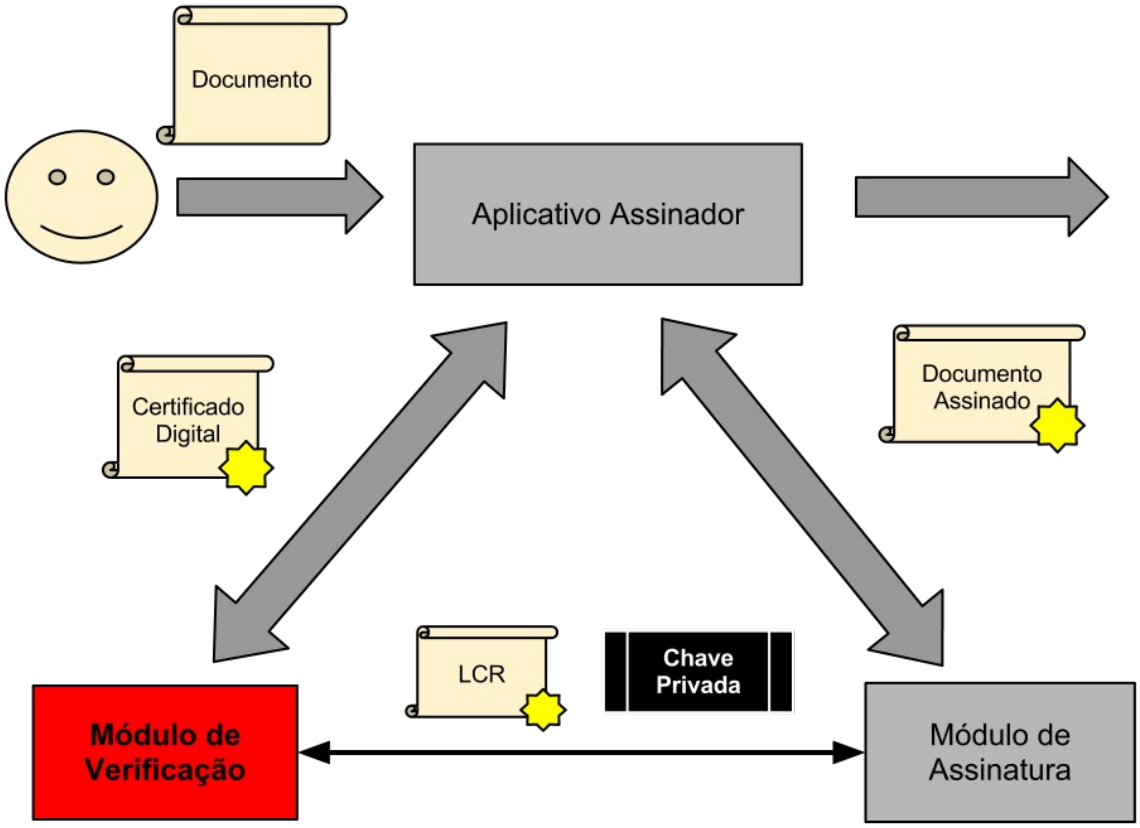


Figura 15 - Aplicativo Assinador
Fonte : Autoria Própria

Para demonstrar o funcionamento do módulo de verificação, foram realizados alguns

diagramas de classes, estes foram realizados de forma superficial para tonar o processo de entendimento mais simples.

O primeiro diagrama a ser apresentado é o da figura 16, este demonstra a dependência existente entre as classes de validação de assinatura (*ICPBrasilSignedData; ICPBrasilTimeStamp*) e de certificados (*ICPBrasilCertificate*). A classe de validação de certificados possui uma dependência do repositório de certificados (*ICPBrasilStore*), sendo assim as classes de validação de assinatura possuem uma dependência indireta das classes responsáveis pelo repositório.

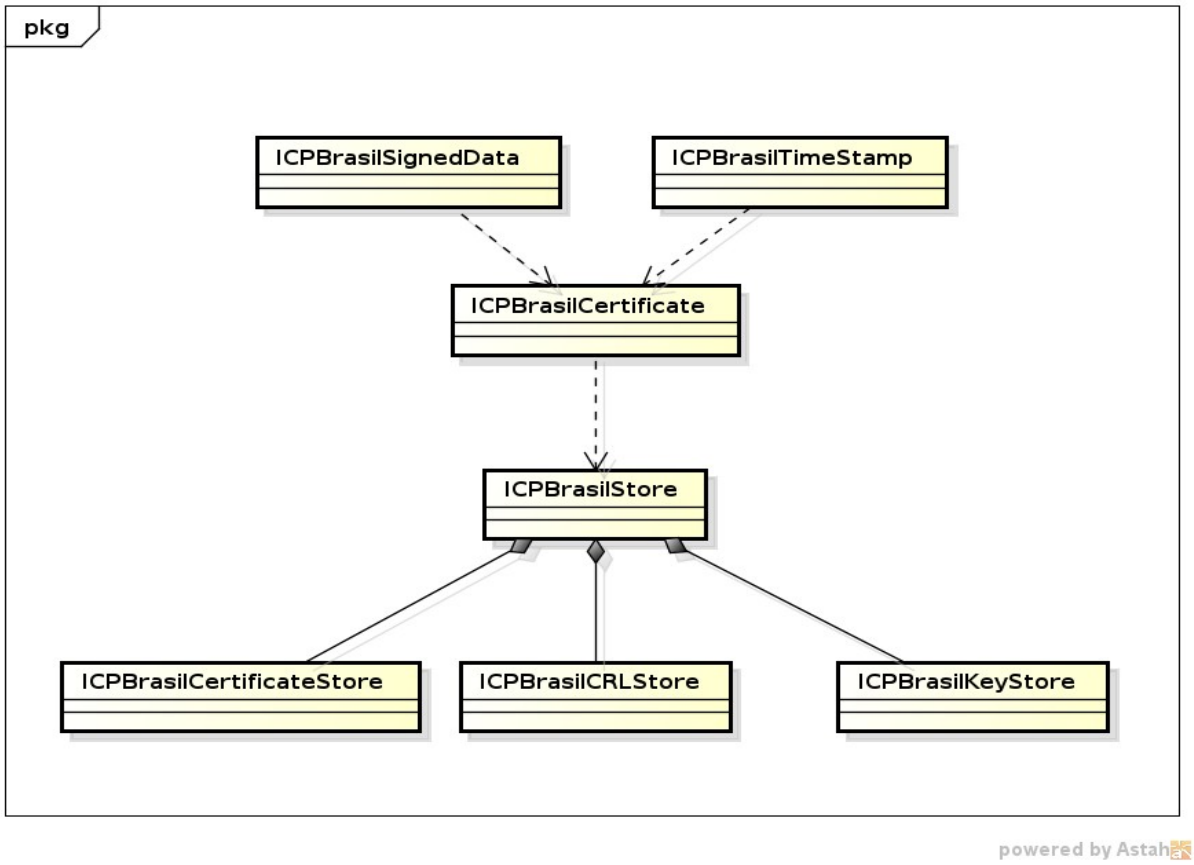


Figura 16-Diagrama de classes Repositório

Fonte : Autoria Própria

Para a validação dos certificados foi implementada a estrutura de classes apresentada na figura 17, esta estrutura separa bem os tipos de certificados definidos pelas politicas ICP-Brasil, tornando os processos de validações independentes. Os métodos que realizam validações genéricas foram reaproveitados através da herança.

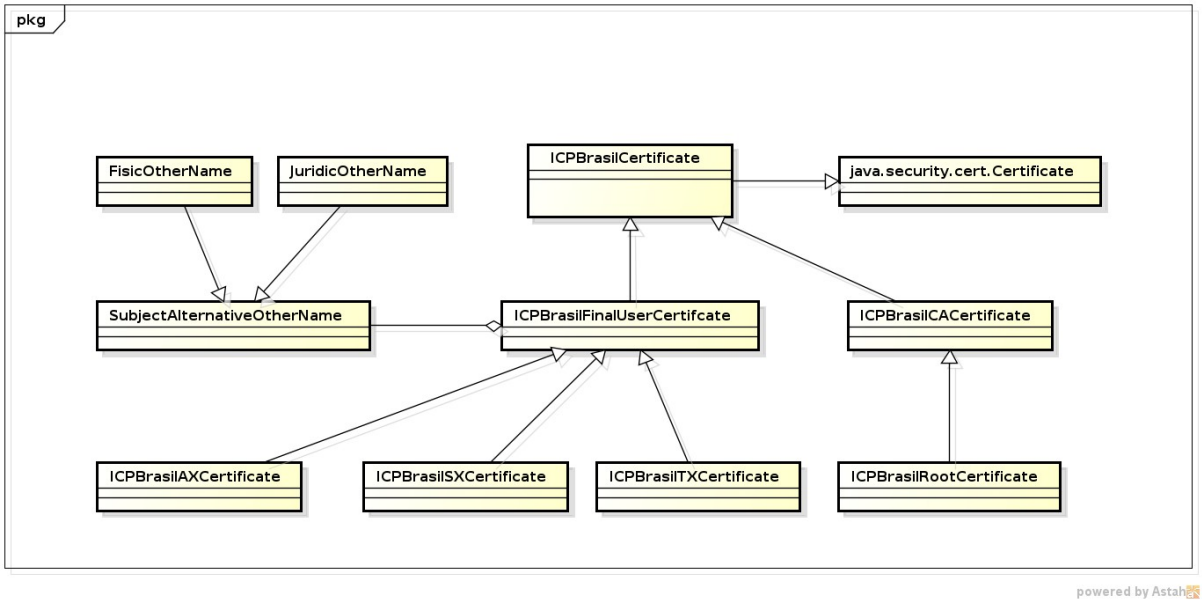


Figura 17- Diagrama de Classes validação de certificado

Fonte : Autoria Própria

A figura 18 apresenta a estrutura de classes para a validação de CMSs e carimbos de tempo.

Assim como a estrutura de classes utilizada na validação de certificados os padrões de assinatura se relacionam com herança, reaproveitando os métodos de validação genéricos.

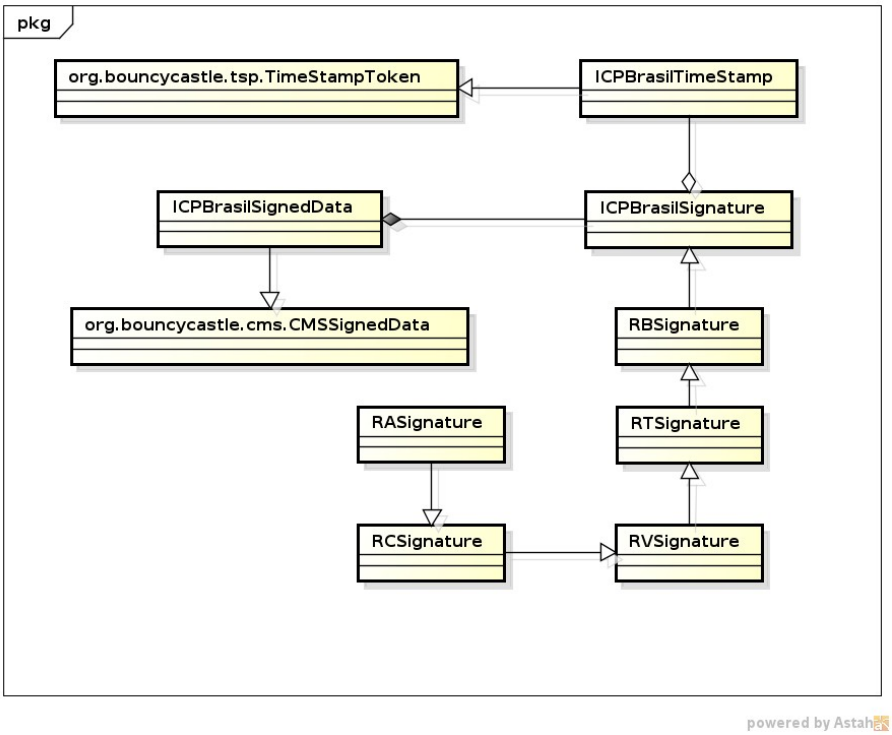


Figura 18-Diagrama de classes validação de assinaturas

Fonte : Autoria Própria

## 5.3 Testes

Durante todo o desenvolvimento foram realizados testes singulares do sistema, para que assim fosse assegurado que os recursos recém desenvolvidos estivessem cumprindo seu propósito. A realização dos testes foi muito importante no decorrer do projeto já que o desenvolvimento dos módulos estava ocorrendo em paralelo e os recursos precisavam ser compartilhados.

Os testes durante o projeto necessitavam de dados de entrada coerentes ao escopo, eram necessários certificados digitais com uma grande de diversidade de falhas, para que assim elas fossem reconhecidas. A geração dos certificados foi realizada pela empresa LSI-TEC, junto a uma tabela de anomalias para serem reconhecidas.

Na figura 19 é apresentado a verificação de um certificado que não contem anomalias, porem suas ACs possuem alguns valores incorretos , criando uma anomalia para o certificado. Na figura 20 é apresentado um certificado cuja o CPF está incorreto.

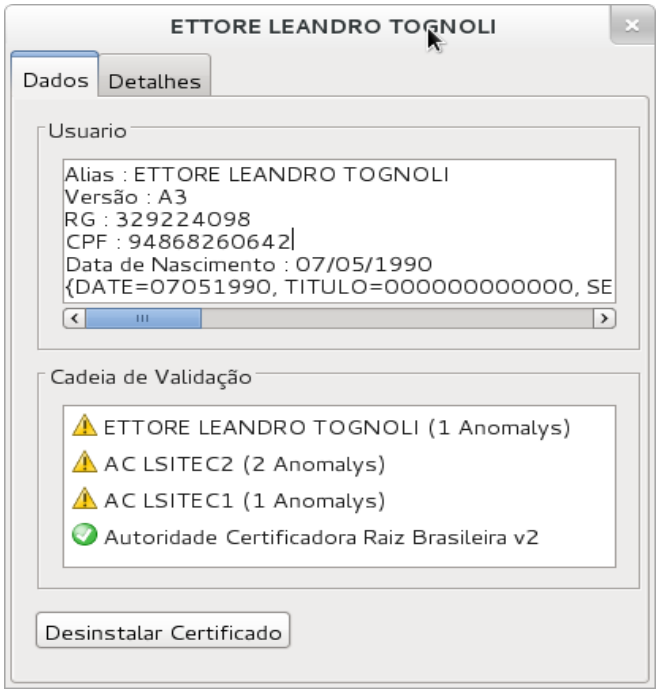


Figura 19-Certificado de Teste 1

Fonte : Autoria Própria

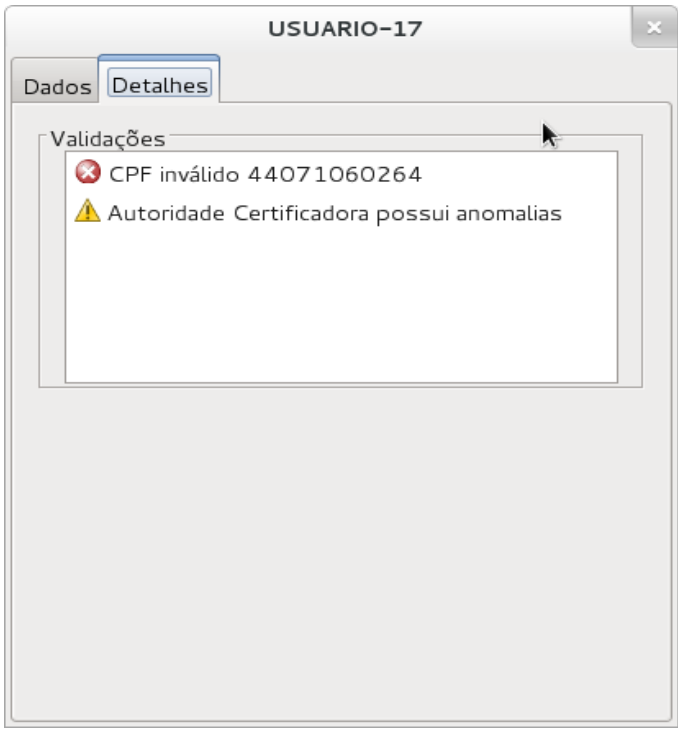


Figura 20-Certificado com CPF Inválido

Fonte : Autoria Própria

Foi utilizado o servidor *Sign Server* para a geração de carimbos de tempo e assim simular as requisições a uma ACT, tornando possível a geração de assinaturas que dependiam dos carimbos de tempo.

Após o desenvolvimento parcial do módulo assinador, tornou-se possível realizar outros testes, agora focados nas verificações de assinatura. Utilizar as assinaturas geradas no próprio UNIVEM foi de muita valia para validar ambos os módulos. Primeiramente os testes foram direcionados para as assinaturas de estrutura mais simples como o padrão AD-RB, posteriormente foram realizados testes com o padrão AD-RT, para que assim fossem validadas as verificações de carimbo de tempo.

Na figura 21 é apresentado um CMS contendo duas assinaturas uma no padrão AD-RB e outra no padrão AD-RA, alguns detalhes da assinatura AD-RA podem ser vistos na figura 22.

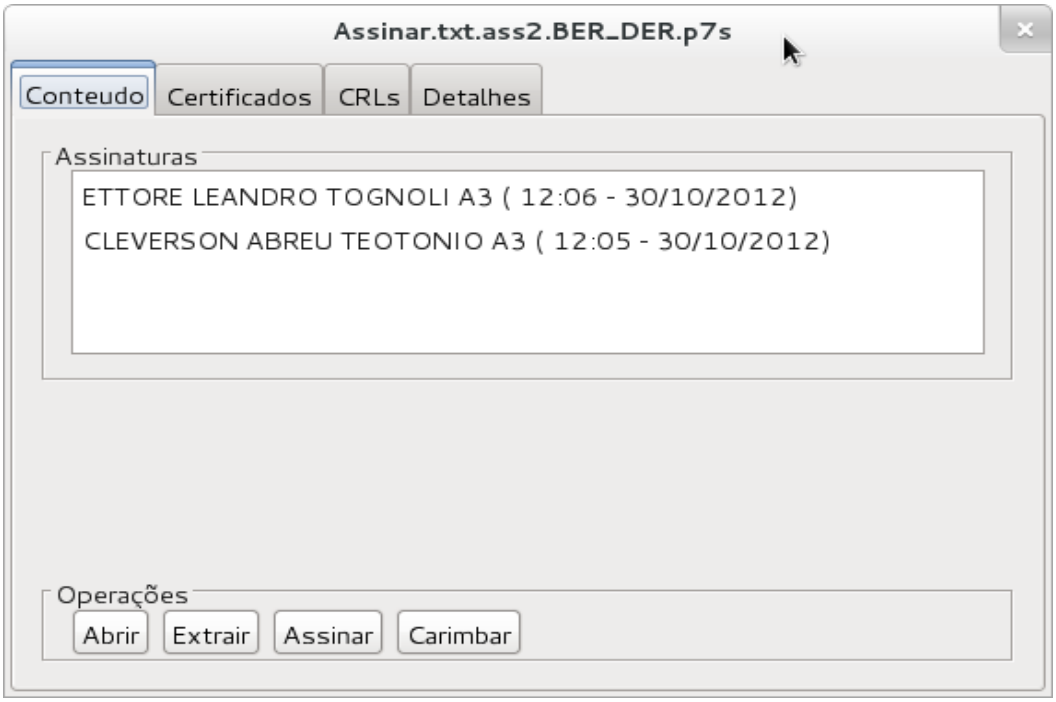


Figura 21 - CMS com assinatura AD-RB e AD-RA

Fonte : Autoria Própria

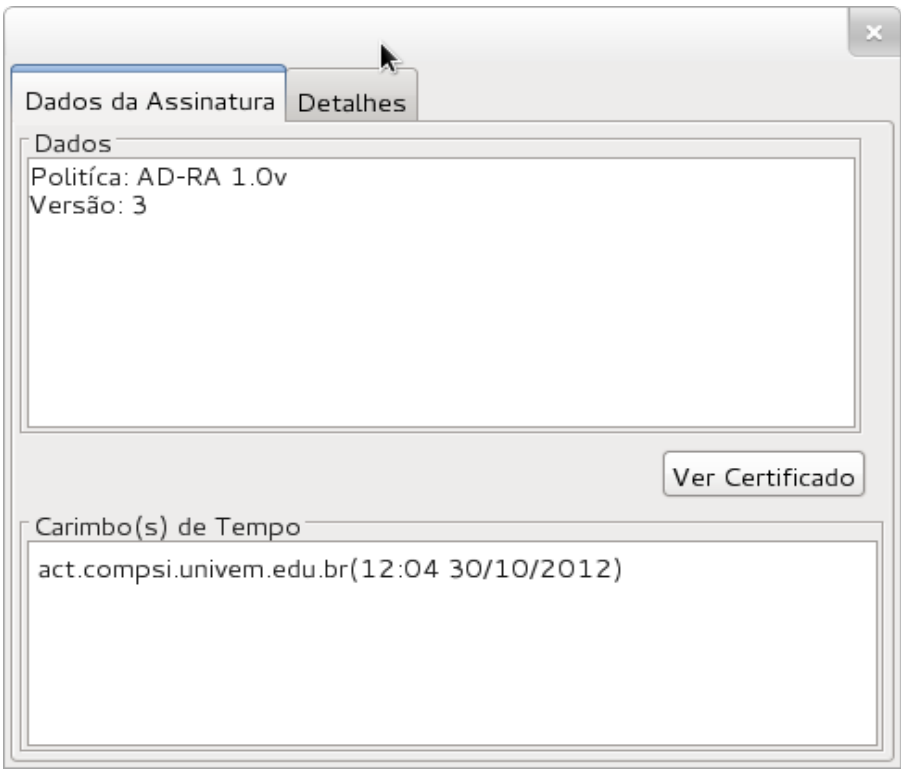


Figura 22-Assinatura AD-RA

Fonte : Autoria Própria

Para que os teste se tornassem mais fieis ao contexto em que o aplicativo seria submetido, foram utilizados certificados das cadeias oficiais da ICP-Brasil.

Na figura 23 é demonstrado uma das telas do aplicativo, esta apresenta os certificados instalados no repositório criado. Pode ser observado que a autoridade Certificadora da Justiça V4 encontra-se invalida, isso é devido a Autoridade Certificadora Raiz Brasileira V2 não ser a verdadeira e sim uma falsa utilizada para testes. As demais cadeias já são os certificados originais.

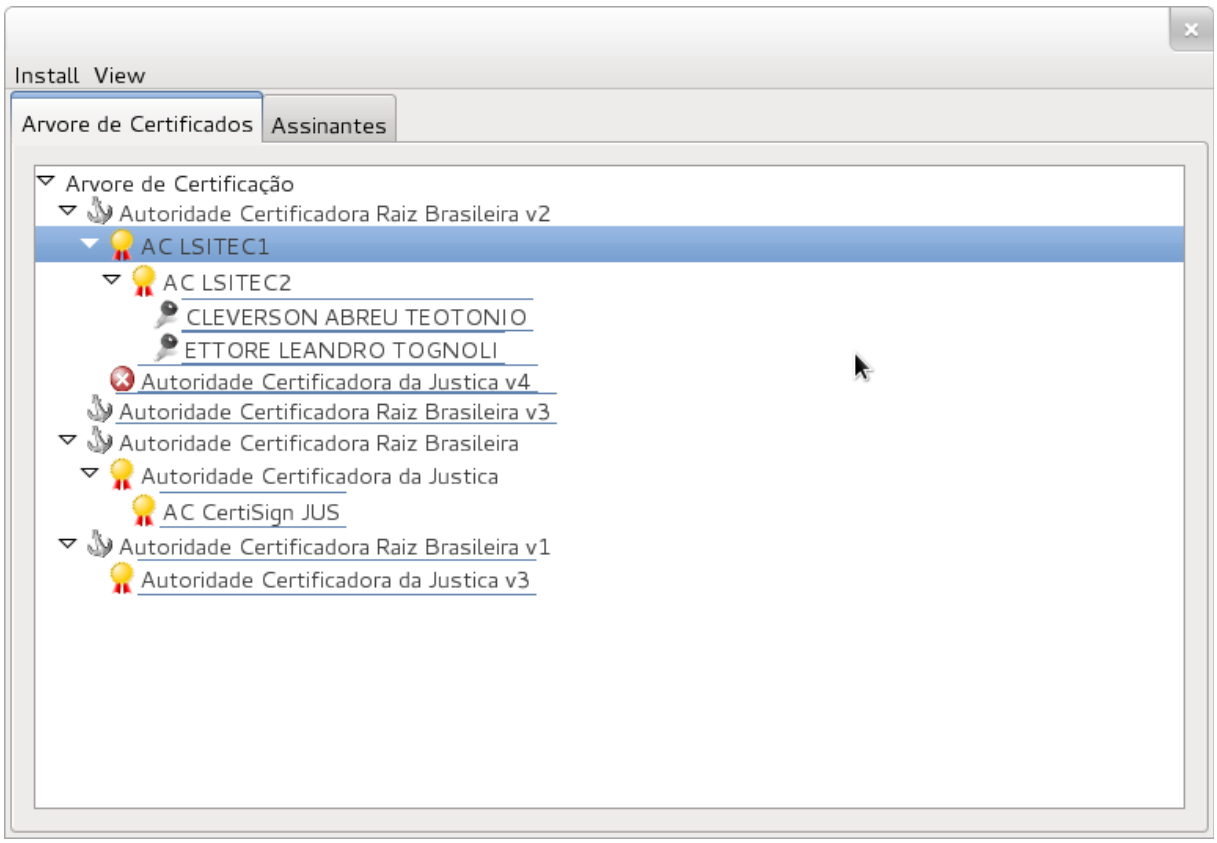


Figura 23-Repositório de Certificados

Fonte : Autoria Própria

# 6. Conclusão

A ICP-Brasil definiu normas minuciosas e de grande valia para garantir a integridade da relação entre chave pública e seu possuidor, utilizou muito bem os campos alternativos definidos pelo padrão X.509 para inserir informações dos documentos do possuidor do certificado. O trabalho realizado pelas autoridades de registro aparentam prevenir muito bem possíveis fraudes no momento da emissão do certificado. Certamente é possível confiar em um certificado pertencente a cadeia da ICP-Brasil.

Entretanto as definições de assinaturas digitais não parecem tão maduras. Para definir o padrão utilizado na assinatura é utilizado um atributo assinado, logo, para trocar-se o padrão definido seria necessário realizar outra assinatura.

Devido a variedade de órgãos regulamentadores tanto nacionais quanto internacionais, foi gerada uma grande quantidade de documentação redundante e também uma descentralização da informação. Algumas especificações da ICP-Brasil aparentam estar abstratas dificultando a implementação de forma precisa.

Foi então desenvolvida com sucesso uma API de verificação de assinaturas digitais. Esta API de verificação de assinaturas e certificados digitais, contempla todas as políticas de usuário final da ICP-Brasil (A1, A2, A3, A4, S1, S2, S3, S4, T3, T4 ) e realiza verificações em toda cadeia de AC. Abrange de forma genérica todos os formatos de assinaturas.

A implementação de todas normas da ICP-Brasil é um trabalho minucioso e exige muita organização do código e da modelagem. Como trabalhos futuros, a implementação da API apresentada nesta monografia pode e deve ser melhorada a fim de torna-la mais eficaz e flexível.

A API de verificação não está preparada para atender novos tipos de certificados e assinaturas que possam surgir, sem que aja uma modificação no código fonte. Deve ser considerado a definição de um arquivo que aponte as validações necessárias, este arquivo deveria ser assinado pela ICP-Brasil para que estas validações sejam autenticas. Com essa definição poderia ser desenvolvido um validador mais dinâmico.

Alguns trechos do código necessitam de refatoração para padrões de projeto, tornando mais simples a manutenção e auxiliando o *software* a se tornar mais flexível e dinâmico.

## Referências Bibliográficas

MORENO, Edward David; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em Software e Hardware**. 1.ed. São Paulo: Novatec Editora Ltda., 2005.

ICP-Brasil. **Requisitos para Geração e Verificação de Assinaturas Digitais na ICP-Brasill – DOC-ICP-15.01** – Versão 2.0 . Brasil. 2010.

Ignaczak, Luciano. **Um Novo Modelo de Infra-estrutura de Chaves Públicas para Uso no Brasil Utilizando Aplicativos com o Código Fonte Aberto** .Florianópolis,Dissertação submetida a Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação.2002.

Fiarresga , Victor Manuel Calhabrês. **Criptografia e Matemática** . Dissertação submetida a Faculdade de Ciências da Universidade de Lisboa ,Mestrado em Matemática para Professores . 2010.

GUELFI, Adilson Eduardo. **Apresentações de slides utilizadas na ministração de treinamento em processos e conceitos pertinentes a assinatura digital no Brasil**. Marília, 2012.

Barra , Marcello Cavalcanti. **INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA (ICP-BRASIL) E A FORMAÇÃO DO ESTADO ELETRÔNICO** .Brasília, Dissertação apresentada ao Departamento de Sociologia da Universidade de Brasília/UnB como parte dos requisitos para a obtenção do título de Mestre..2006.

SQLite, **SQLite home page,** disponível em <http://www.sqlite.org>. Acessado em outubro de 2012

STALLINGS, William. **Criptografia e segurança de redes**. 4a ed. São Paulo, Pearson, 492p. 2008.

SIGNE SERVER, **SIGN SERVER home page**, disponível em <http://ww.signserver.org>.

Acessado em setembro de 2012.

ITI , **ITI home page**, disponível em <http://www.iti.gov.br>, acessado em outubro de 2012.