UNICEUB – CENTRO UNIVERSITÁRIO DE BRASÍLIA

FAET - FACULDADE DE CIÊNCIAS EXATAS E TECNOLOGICAS

CURSO DE ENGENHARIA DA COMPUTAÇÃO

O USO DE CERTIFICADOS DIGITAIS ICP BRASIL, PADRÃO A3, COMO TECNOLOGIA DE ACESSO A CONTA-CORRENTE EM CANAL DE AUTO-ATENDIMENTO INTERNET

HENRIQUE CEZAR MARTINS LEONCIO

BRASÍLIA – DF
2006

HENRIQUE CEZAR MARTINS LEONCIO

O USO DE CERTIFICADOS DIGITAIS ICP BRASIL, PADRÃO A3, COMO TECNOLOGIA DE ACESSO A CONTA-CORRENTE EM CANAL DE AUTO-ATENDIMENTO INTERNET

Monografia apresentada ao Centro Universitário de Brasília – UniCEUB como um dos pré-requisitos para obtenção do título de Bacharel em Engenharia da Computação.

Prof. Orientador: Msc. Marco Antônio Araújo

Brasília-DF, julho de 2006

HENRIQUE CEZAR MARTINS LEONCIO

O USO DE CERTIFICADOS DIGITAIS ICP BRASIL, PADRÃO A3, COMO TECNOLOGIA DE ACESSO A CONTA-CORRENTE EM CANAL DE AUTO-ATENDIMENTO INTERNET

Monografia apresentada ao Centro Universitário de Brasília – UniCEUB como um dos pré-requisitos para obtenção do título de Bacharel em Engenharia da Computação.

MEMBROS DA BANCA EXAMINADORA

MEMBROS DA BANCA	**ASSINATURA**
1. COORDENADOR DO CURSO Prof.:	
2. PROFESSOR ORIENTADOR Prof.:	
3. PROFESSOR (A) EXAMINADOR Prof.:	
4. PROFESSOR (A) EXAMINADOR Prof.:	
5. PROFESSOR CONVIDADO Prof. :	

Brasília/DF, ... de ..... de 2006

Dedicatória

A minha grande mãe, Ceberina Martins Leoncio, e ao meu grande pai, Milton Leoncio, pelo amor, exemplo e apoio ao longo destes anos.

A minha amada esposa, Juliana, pelo incentivo e apoio incondicional em todos os momentos.

Aos meus irmãos, Gustavo e Jackeline, pelo carinho e palavras amigas.

Agradecimentos

A Deus, pela vida, pela família e pela esposa que me deu.

Ao meu Orientador, professor Marco Antônio, por acreditar neste trabalho e pelas sábias dicas e sugestões, fundamentais para a conclusão do mesmo.

Ao amigo Jorge André Benedetti, pelas valiosas dicas e incentivo.

Ao colega Bruno de Melo Silva, pelas palavras de apoio e ajuda em todas as etapas deste trabalho.

Ao colega Mário Márcio Monteiro Linhares, pela auxílio no desenvolvimento das páginas HTML.

A todos os colegas e professores pela convivência e aprendizado ao longo desses anos.

Lista de figuras

FIGURA 1 - Teclado virtual do Banco do Brasil..... 16
FIGURA 2 - Teclado virtual do Banco Bradesco..... 17
FIGURA 3 - Teclado virtual do Banco Itaú..... 17
FIGURA 4 - Teclado virtual do Banco Unibanco..... 18
FIGURA 5 - Teclado virtual da Caixa Econômica Federal..... 18
FIGURA 6 - Falsa interface do teclado virtual do Banco do Brasil..... 25
FIGURA 7 - Falsa interface do teclado virtual do Banco Bradesco..... 25
FIGURA 8 - Falsa interface do teclado virtual da Caixa Econômica Federal..... 25
FIGURA 9 - Página falsa do Banco do Brasil..... 26
FIGURA 10 - Página falsa do Banco Itaú..... 27
FIGURA 11 - Infra-estrutura da ICP Brasil e suas principais entidades..... 32
FIGURA 12 - Estrutura do certificado X.509v3..... 35
FIGURA 13 - Criptografia Assimétrica utilizada para garantir a confidencialidade..... 36
FIGURA 14 - Criptografia Assimétrica utilizada para garantir a autenticidade..... 37
FIGURA 15 - Assinatura digital utilizando criptografia assimétrica..... 38
FIGURA 16 - Conferência da Assinatura Digital..... 38
FIGURA 17 - Etapas para aquisição de Certificados Digitais ICP Brasil..... 40
FIGURA 18 - Smart Card com CPU..... 43
FIGURA 19 - Elementos de um smart card..... 45
FIGURA 20 - Leitoras de smart cards (marcas Perto e Gemplus respectivamente)..... 46
FIGURA 21 - Tokens USB..... 47
FIGURA 22 - Leiaute dos cartões e-CPF e e-CNPJ..... 51
FIGURA 23 - Certificado utilizado na simulação..... 53
FIGURA 24 - Interface da ferramenta utilizada para o gerenciamento do cartão..... 54
FIGURA 25 - Cadeia de Raízes..... 55
FIGURA 26 - Principais informações do certificado armazenadas no banco de dados..... 57
FIGURA 27 - Fluxograma lógico das validações realizadas..... 58
FIGURA 28 - Página HTML utilizada para representar o site de um banco qualquer..... 62
FIGURA 29 - Página HTML utilizada para carregar a applet de autenticação..... 62
FIGURA 30 - Página HTML apresentada após a liberação do acesso..... 63

Lista de tabelas

Tabela 1 - Tipos de Certificados ICP Brasil..... 33
Tabela 2 - Preços de certificados digitais ICP Brasil do tipo A3 e-CPF..... 51

Lista de siglas

AC - Autoridade Certificadora
AR - Autoridade de Registro
CSP Cryptographic Service Provider
DPC - Declaração de Práticas de Certificação
PC - Política de Certificação
ICP - Infra-estrutura de Chaves Públicas
FTP - File Transfer Protocol
ITI - Instituto Nacional de Tecnologia da Informação
IRC - Internet Relay Chat
LCR - Lista de Certificados Revogados

Resumo

Neste trabalho serão avaliados os principais mecanismos de segurança para acesso aos serviços de *internet banking*, de alguns dos maiores bancos do país, bem como as vulnerabilidades dessa tecnologia, conhecida como teclado virtual, e os riscos a que os usuários desses serviços estão sujeitos ao acessarem sua conta-corrente pela *internet*. Após essa análise, visando agregar mais segurança no acesso e autenticação dos clientes, será proposto um novo método de autenticação, baseado no uso de Certificados Digitais ICP Brasil, padrão A3.

Esse novo método consiste em substituir as atuais senhas de acesso utilizadas pelos usuários de serviços bancários de auto-atendimento *internet*, bem como a atual tecnologia de teclado virtual, hoje utilizada pela maioria dos bancos no país, por uma solução capaz de validar o cliente, titular de um Certificado Digital do tipo A3, emitido no âmbito da Infra-estrutura de Chaves Públicas Brasileira (ICP Brasil). Com essa solução será possível aumentar sensivelmente o nível de segurança dos clientes que utilizam esses serviços, além de permitir a redução do volume de fraudes que as instituições financeiras têm nesse canal.

Esses certificados podem ser armazenados em *tokens* criptográficos USB ou em *smart cards*. Por motivo de simplificação e redução de custo, optou-se por trabalhar com um certificado armazenado em *smart card*.

Certificados A3 são atualmente uma das tecnologias mais seguras disponíveis para a realização de transações em rede, pois com os recursos computacionais atuais, é praticamente impossível quebrar ou obter a chave privada vinculada a esses certificados.

É importante destacar que os certificados digitais não serão emitidos pela instituição financeira, esta apenas aceitará a utilização de Certificados ICP Brasil (A3) por seus clientes para acesso a conta-corrente pela *internet*.

Palavras-chave: ICP Brasil, *internet banking*, certificados digitais, *smart card* e *tokens* criptográficos USB.

Abstract

This project will focus on the main mechanisms of internet banking security of the biggest banks in Brazil and some of vulnerabilities of this technology known as virtual keyboard. We will cover the risk posed to these users while browsing to their count-chain. The purpose is to give more security on client authentication process. Therefore it will be purposed a new authentication method based on standard A3 ICP-Brazil digital certificates.

This new method consist in changing the current passwords used by internet service banking and the virtual keyboard that are still used by most of the banks in this country. The new solution will be capable to validate the client with its own A3 Digital Certificate emitted from Brazilian Public Keys (ICP-Brazil). This solution will proportionate a higher security level to the clients and will reduce the frauds posed to the financial institutions.

These certificates can be stored in USB cryptographic tokens or on smart cards. To reduce the cost was decided to work with the certificate stored on smart card.

Today A3 Certificates are one of the most security technology to work with internet transactions because it is impossible to take the private key of these certificates with the computer resources existing nowadays.

It is important to detach that digital certificates will not be emitted by financial institutions. These corporations will accept the use of ICP-Brazil (A3) certificates by their clients to give access to the count-chain with the internet.

Keywords: ICP-Brazil, Internet banking, Digital Certificates; smart card and criptographic USB tokens.

Sumário

1. Introdução..... 12

1.1 Objetivos..... 12

1.1.1 Objetivo Geral..... 12

1.1.2 Objetivos Específivos..... 13

1.2 Trabalhos correlatos..... 13

1.3 Motivação..... 14

2. Serviços de Internet Banking..... 16

2.1 Exemplos de acesso aos serviços de Internet Banking..... 16

2.1.1 Banco do Brasil..... 16

2.1.2 Banco Bradesco..... 17

2.1.3 Banco Itaú..... 17

2.1.4 Banco UNIBANCO..... 18

2.1.5 Banco Caixa Econômica Federal..... 18

2.2 Métodos de Autenticação..... 19

2.2.1 Algo que você sabe..... 19

2.2.2 Algo que você tem..... 20

2.2.3 Algo que você é..... 20

2.3 Teclado virtual..... 21

3. Riscos e vulnerabilidades dos usuários de serviços de internet banking..... 23

3.1 Tipos de códigos maliciosos ou malwares..... 23

3.1.1 Vírus..... 23

3.1.2 Cavalo-de-Tróia e Backdoor..... 24

3.1.3 Worms e Bots..... 28

3.1.4 Spyware e Adware..... 28

3.2 Formas de Proteção..... 29

4. Certificados Digitais ICP Brasil..... 31

4.1 A ICP Brasil..... 31

4.2 Obrigações da Terceira Parte..... 32

4.3 Tipos de Certificados Digitais na ICP Brasil..... 32

4.4 O padrão X.509..... 34

4.5 Características do certificado..... 36

4.5.1 Criptografia Assimétrica..... 36

4.5.2 Assinatura Digital..... 37
5. Processo de Emissão de Certificados Digitais ICP Brasil..... 39
6. O uso de Certificados Digitais ICP Brasil no país..... 42
7. Dispositivos de armazenamento e portabilidade de certificados digitais..... 43
7.1 Smart Cards..... 43
7.1.1 Vantagens dos smart cards..... 44
7.1.2 Leitoras de smart cards..... 46
7.2 Tokens..... 46
7.2.1 Tokens USB..... 47
7.3 Diferenças entre tokens USB e smart cards..... 47
8. Solução proposta..... 49
8.1 Requisitos funcionais da aplicação..... 49
8.2 O certificado e o smart card escolhidos para o trabalho..... 50
8.3 O desenvolvimento da aplicação..... 52
8.3.1 Computador e Sistema Operacional utilizados..... 52
8.3.2 Características do certificado utilizado..... 53
8.3.3 Driver da Leitora e CSP do cartão..... 54
8.3.4 Instalação da Cadeia de Raízes..... 55
8.3.5 Pré-requisitos para a solução proposta..... 56
8.3.6 A aplicação Java utilizada para autenticação do usuário..... 58
8.3.7 As páginas HTML..... 61
8.3.8 O servidor web utilizado..... 63
8.3.9 Dificuldades encontradas e suas soluções..... 64
8.4 Vantagens e desvantagens da solução proposta..... 64
9. Conclusão..... 66
10 Trabalhos Futuros..... 67
11 Referências Bibliográficas..... 68
Anexos..... 72
Anexo A - Código Fonte da Applet Java..... 72
Anexo B - Código Fonte dos métodos de autenticação..... 75

1. Introdução

Com o surgimento da *internet*, as instituições financeiras de todo o mundo, passaram a vislumbrar um novo mercado para seus negócios, onde poderiam prover novos serviços e reduzir seus custos operacionais. No Brasil não foi diferente e, há poucos anos os bancos passaram a fornecer a seus clientes a comodidade e as facilidades do banco pela internet ou *internet banking*, que possibilitou a replicação de grande parte dos serviços, antes disponíveis somente na rede de agências, para o mundo virtual. Além disso, a cada ano vem ocorrendo um incremento no número de serviços disponíveis nesse canal, a tal ponto que hoje, salvo algumas exceções ou restrições como saque e retirada de cheques, serviços como transferências, empréstimos, pagamentos e até recarga de celular já podem ser feitos pela *internet* nos *sites* dos grandes bancos do país. Entretanto, paralelamente a esse crescimento, também aumentou a quantidade de programas maliciosos que circulam na *internet*, sendo que alguns desses programas foram criados especificamente para capturar dados de usuários de serviços de *internet banking*.

Visando reduzir as perdas financeiras, o risco de imagem e o desgaste com seus clientes, os bancos têm feito grandes investimentos na área de segurança.

Porém, apesar dos altos investimentos dos bancos, as fraudes nesse canal não estão reduzindo na velocidade desejada, o que preocupa tanto os usuários, principais beneficiários dessa comodidade, quanto as instituições financeiras, que a cada dia precisam redobrar seus cuidados, além de procurar manter um equilíbrio entre a facilidade de uso e a segurança dessas soluções, pois uma solução que seja difícil de utilizar, em função de inúmeras exigências, não terá boa aceitação pelos clientes.

Buscando obter mais segurança, os bancos têm estudado outras soluções e o uso de certificados digitais é uma delas.

1.1 Objetivos

1.1.1 Objetivo Geral

O objetivo geral desta monografia é apresentar uma nova forma de acesso a serviços de *internet banking* baseada na utilização de Certificados Digitais ICP Brasil do tipo A3 por clientes de instituições financeiras. Com isso pretende-se mostrar a utilização

desses certificados, como alternativa ou complemento à tecnologia de teclado virtual e de senhas compartilhadas atualmente adotada pelos bancos.

1.1.2 Objetivos Específicos

Para atingir os objetivos gerais os seguintes objetivos específicos devem ser alcançados:

- Apresentar as formas de autenticação a serviços de *internet banking* utilizadas pelos principais bancos do país;
- Apresentar as vulnerabilidades dos teclados virtuais para os usuários desses serviços;
- Discorrer sobre a ICP Brasil e Certificados Digitais;
- Discorrer sobre o processo de emissão de Certificados Digitais na ICP Brasil;
- Apresentar os principais dispositivos de armazenamento e portabilidade de Certificados Digitais do tipo A3;
- Implementar uma solução que simule o acesso ao serviço de *internet banking* de um banco qualquer com a utilização de um Certificado Digital ICP Brasil do tipo A3.

1.2 Trabalhos correlatos

Durante os últimos anos o tema certificação digital vem ganhando importância em várias áreas relacionadas à segurança, seja no tráfego de informações em rede, seja no processo de assinatura digital de documentos, motivando desta forma trabalhos em diversas áreas afins. **[1] [2] [3]**

Um importante trabalho, utilizado como referência para a elaboração deste, foi apresentado em 2004 por alunos do curso de Engenharia Elétrica da Universidade de Brasília, como requisito para obtenção do grau de Engenheiro de Redes. Ele trata da Autenticação de Usuários em Serviços Web de Instituições Financeiras, porém com uma abordagem diferenciada, em que é proposto um novo modelo de teclado virtual. **[4]**

1.3 Motivação

Devido ao risco de imagem e a conseqüente perda de credibilidade que a divulgação de informações referentes a fraudes nos canais de auto-atendimento dos bancos podem causar, estes mantêm sobre total sigilo esses dados. Entretanto, segundo matéria divulgada, em 25 de abril de 2005 pelo jornal Valor on-line, sob o título *"Crescem fraudes a bancos na internet",* os crimes cibernéticos provocaram perdas de US$ 1,4 trilhão para os internautas em todo o mundo no ano de 2004, sendo que as fraudes bancárias e financeiras estão entre as que mais crescem, tanto que, no mesmo ano avançaram 578% em relação a 2003 e no primeiro trimestre de 2005, registraram um aumento de 178% em comparação com o mesmo período de 2004. Esses números podem ainda ser maiores, pois os responsáveis pela pesquisa trabalham apenas com relatos voluntários. No ranking geral de ocorrências, o Brasil ocupa a segunda posição, com 26,14% do total dos relatos, atrás dos Estados Unidos, com 27,62%. **[5]**

Segundo a mesma matéria, os *hackers* já roubam mais dos bancos que os assaltantes de agências e, para se ter um idéia desse volume, na Operação Matrix, de fevereiro de 2005, e na Operação Cavalo de Tróia II, de 2004, duas quadrilhas presas pela Polícia Federal podem ter desviado mais de R$440 milhões dos bancos. De acordo com um estudo da Polícia Federal Americana (FBI), em um assalto a banco são roubados, em média, US$ 15 mil, e os assaltantes têm 75% de chance de serem presos. Já num "assalto na internet", o roubo médio é de US$ 1 milhão e o risco de prisão é de 5%.

O retorno que a fraude proporciona a esses criminosos é um dos fatores que explica o aumento das ocorrências, outro é a rápida disseminação das técnicas de ataque.

Como não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição financeira, os atacantes concentram seus esforços na exploração das fragilidades dos clientes dos bancos, usuários desses serviços pela internet. Esses criminosos aproveitam-se do desconhecimento e da falta de cuidados básicos que não são adotados pelos usuários para conseguir o que desejam.

A principal tecnologia atualmente adotada pelos bancos para acesso aos seus serviços de *internet banking* são os teclados virtuais, que dependendo da instituição financeira, podem se apresentar de várias maneiras ao cliente. Alguns bancos têm adotado variações desses teclados combinadas com outras soluções de segurança.

Circula, pela internet, uma enorme variedade e quantidade de programas maliciosos utilizados para ludibriar os usuários de serviços bancários na internet, entre esses programas destacam-se os chamados cavalos-de-tróia ou *“trojans horse”*. Esses programas, quando instalados no computador do cliente, usuário de um banco on-line, passam a monitorar suas atividades na internet. Dessa forma, quando o usuário acessa o *site* de seu banco, surge para ele uma falsa página de login, às vezes perfeitamente idêntica à página original, solicitando que o mesmo informe os dados de sua conta-corrente, como número da agência, número da conta-corrente e senha.

De posse dessas informações, o atacante passa a ter acesso à conta do usuário e pode realizar todas as movimentações financeiras possíveis, agindo como se fosse o titular da conta. Entre as principais transações, destacam-se aquelas que envolvem valor, como transferência entre contas, pagamentos de títulos e recarga de celular pré-pago.

Alguns cavalos-de-tróia atuam de maneira que o usuário pode ter suas informações furtadas mesmo quando visitam o *site* verdadeiro do banco.

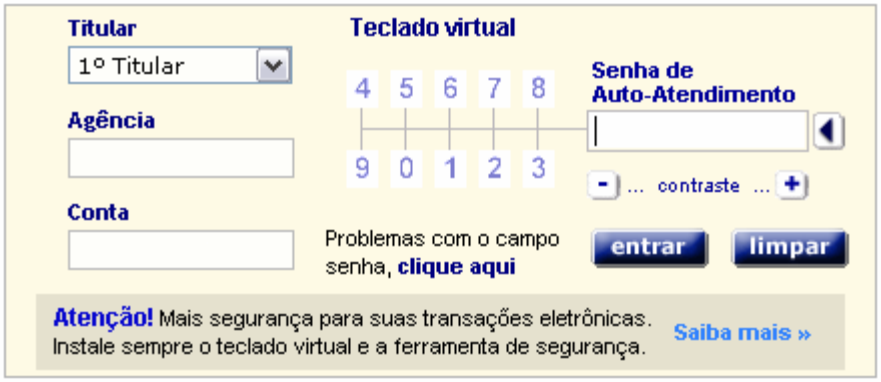
2. Serviços de *Internet Banking*

A utilização do canal internet para realização de transações financeiras teve início por volta de 1996, época em que os grandes bancos do País começaram a oferecer a seus clientes os primeiros serviços por esse canal **[2]**. A utilização da internet, para a realização de transações que antes só eram realizadas nos guichês de caixa ou nos terminais de auto-atendimento, permitiu aos bancos reduzirem seus custos na prestação desses serviços. Já os clientes, por sua vez, ganharam comodidade e agilidade por não precisarem mais dirigir-se fisicamente ao seu banco ou a um terminal de auto-atendimento para consultar o saldo de sua conta-corrente ou realizar um pagamento.

2.1 Exemplos de acesso aos serviços de *Internet Banking*

2.1.1 Banco do Brasil

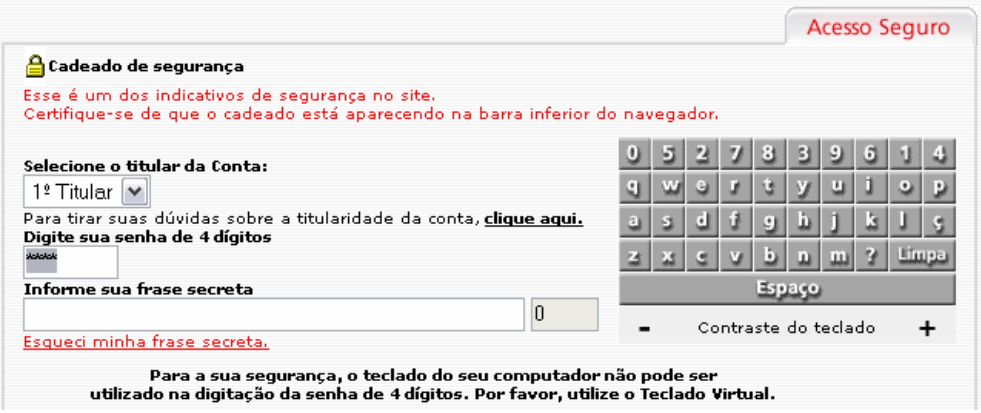
O cliente do Banco do Brasil, para acessar sua conta-corrente pela internet precisa informar, além do prefixo da agência e número da conta-corrente, que devem ser digitados por meio do teclado convencional, uma senha numérica de oito dígitos via teclado virtual, conforme mostrado na figura abaixo.



Fonte: https://www2.bancobrasil.com.br/aapf/aai/login.pbk?url=idh/termoAAPF.jsp
Figura 1 – Teclado virtual do Banco do Brasil

2.1.2 Banco Bradesco

O cliente do Banco Bradesco, para acessar sua conta-corrente pela internet precisa informar, além do prefixo da agência e do número da conta-corrente, digitados via teclado convencional na página principal do banco, uma senha numérica de quatro dígitos que é informada por meio do teclado virtual mostrado na **figura 2**. Em complemento a senha, também é preciso informar uma frase secreta previamente cadastrada.



Fonte: http://www.bradesco.com.br/
Figura 2 – Teclado virtual do Banco Bradesco

2.1.3 Banco Itaú

O cliente do Banco Itaú, para acessar sua conta-corrente pela internet precisa informar, também pela utilização do mouse via teclado virtual, um senha numérica de seis a oito dígitos. Porém neste caso, ao contrário do que foi mostrado até agora, a opção dos dígitos é apresentada por meio de cinco botões com dois números cada.

Fonte: http://www.itau.com.br/indexNE6.htm
Figura 3 – Teclado virtual do Banco Itaú

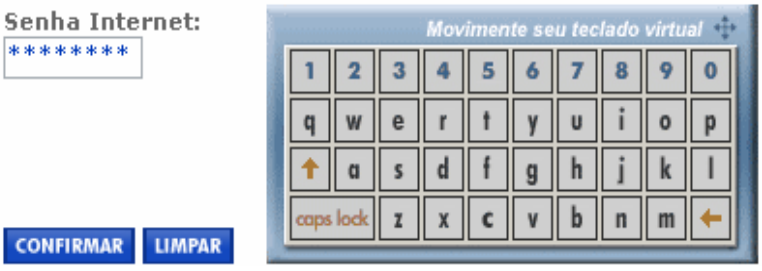
2.1.4 Banco UNIBANCO

Para acesso ao *internet banking* do Unibanco, o cliente precisa informar uma senha numérica de quatro dígitos. Seu teclado virtual possui quatro botões, sendo que cada botão representa três números diferentes. Esses botões mudam de posição a cada acesso do usuário, entretanto os números associados a cada botão são sempre os mesmos. Outro detalhe importante desta solução é que um mesmo número pode aparecer em dois botões distintos, como é o caso do número 1, mostrado na **figura 4**. Neste caso, se a senha for composta pelo número 1, ele pode ser escolhido em qualquer um dos dois botões.

Fonte: http://www.unibanco.com.br/hom/index.asp
Figura 4 – Teclado virtual do Banco Unibanco

2.1.5 Banco Caixa Econômica Federal

O *internet banking* da Caixa Econômica Federal é acessado por meio da utilização de uma senha alfanumérica de seis posições, informada via um teclado virtual muito semelhante a um teclado convencional. Um exemplo deste teclado é mostrado na **figura 5**.



Fonte: http://www.caixa.gov.br/
Figura 5 – Teclado virtual da Caixa Econômica Federal

2.2 Métodos de Autenticação

A identificação de um usuário e sua autenticação com segurança são premissas básicas para uma instituição financeira permitir o acesso por parte de seus clientes ao seu serviço de *internet banking.* A identificação diz a um sistema quem você é, enquanto que a autenticação provê um mecanismo eficiente de provar que você realmente é quem diz ser.

Por isso, a autenticação precisa ser feita com base em alguma característica que somente o usuário identificado seja capaz de fornecer. As principais formas de validação de autenticidade são baseadas nos seguintes conceitos: **[6]**

- “Algo que você sabe”;
- “Algo que você tem”;
- “Algo que você é”.

Dependendo da finalidade a que se destina e do nível de segurança que se requer para uma aplicação, cada um desses métodos apresenta vantagens e desvantagens.

2.2.1 Algo que você sabe

O exemplo mais comum neste caso é o uso de senhas ou PINs, como as senhas para acesso à caixa postal de e-mail, senhas bancárias, senhas utilizadas no local de trabalho para se obter acesso a determinado sistema, etc. Apesar de ser o método de autenticação mais usado e mais antigo, ele contém uma série de deficiências que não o torna muito confiável. A principal é que ele se baseia na capacidade dos usuários de memorizar inúmeras senhas, quase sempre de tamanhos e características diferentes. Além do mais, como a maioria das pessoas não têm muita imaginação na hora de criar as senhas, até para evitar esquecê-las facilmente, acabam por criá-las com características de fácil dedução, como nomes, sobrenomes, números de documentos, placas de carros, números de telefones e datas. Outro motivo é que essas senhas podem ser facilmente obtidas por pessoas mal intencionadas com o objetivo de tentar se autenticar como se fossem o titular da senha. Como vantagem para a utilização de senhas, pode-se destacar o baixo custo da sua implementação, pois pode ser usada em qualquer tipo de ambiente, sem a necessidade de hardwares especiais. **[7] [8]**

2.2.2 Algo você tem

Para “algo que você tem”, o exemplo mais conhecido é o uso de cartões magnéticos. Os sistemas de autenticação que se baseiam neste método, utilizam cartões ou *tokens* para validar seus usuários. Os clientes de bancos, para utilizar os terminais de auto-atendimento no acesso a sua conta-corrente, são obrigados a utilizar um cartão associado a uma senha previamente cadastrada. Esses sistemas baseiam-se no fato de que apenas o titular de determinado cartão é quem vai utilizá-lo. As desvantagens desse método são: **[18]**

- Os cartões podem ser facilmente perdidos ou roubados (devido ao seu pequeno tamanho);
- É caro e precisa de hardwares especiais para ler os cartões.

O ponto positivo desse método, se comparado àquele que utiliza somente senhas, é que ele agrega maior nível de segurança às transações, pois considera o uso de cartão e senha ao mesmo tempo. Diante disso, uma pessoa mal intencionada agora precisa, além da senha, também do cartão para poder se passar por alguém.

2.2.3 Algo que você é

O método de autenticação baseado em “algo que você é” está relacionado a biometria, que é um ramo das ciências que estuda a mensuração dos seres vivos **[9]**. A biometria torna possível autenticar um indivíduo a partir de alguma de suas características intrínsecas. Entre todos os métodos de autenticação biométricos atualmente existentes, o mais utilizado é a impressão digital, que consiste na análise feita com base nos desenhos papilares da ponta do dedo. Outras técnicas de biometria também em uso são: **[7] [10]**

- **Face:** toma por base as características faciais. Requer uma câmera digital para a leitura da face.
- **Geometria da mão:** consiste na medição do formato da mão do indivíduo.
- **Íris:** utiliza as características do anel colorido de tecido encontrado ao redor da pupila (o orifício preto do olho).

- **Retina:** envolve a análise da camada de vasos sangüíneos que fica na parte de trás dos olhos. Este método proporciona alta precisão, porém não possui grande aceitação por parte dos usuários, pois exige que os mesmos tenham contato com o mecanismo responsável pelo escaneamento da retina.
- **Voz:** apesar do baixo custo de implementação é a técnica menos confiável. Isto se deve a problemas como ruídos no ambiente e mudanças na voz do usuário, ocasionada, por exemplo, por uma gripe.

A grande vantagem da autenticação por meio de dispositivos biométricos é o fato de ser possível identificar o usuário sem a necessidade deste ter que memorizar senhas ou utilizar cartões. Basta que ele esteja presente e não tenha sofrido algum tipo de acidente na parte do corpo que utiliza para se autenticar.

A principal desvantagem da biometria é que o seu uso depende da aquisição de hardwares especiais para capturar as informações dos indivíduos. Normalmente esses hardwares são muito caros, o que restringe sua utilização a ambientes de alta segurança. Só para se ter uma idéia, um pequeno leitor de impressão digital custa atualmente cerca de R$190,00. **[11]**

2.3 Teclado Virtual

A adoção de teclados virtuais por instituições financeiras surgiu da necessidade de se criar um mecanismo que fornecesse maior segurança aos usuários de *internet banking*, pois as primeiras soluções de autenticação, baseadas na utilização de teclados convencionais, tornaram-se bastante vulneráveis com o tempo devido a ação de programas maliciosos conhecidos por *keyloggers*. Esses programas capturam e armazenam todas as informações digitadas no teclado, inclusive dados bancários.

Os teclados virtuais resolveram os problemas relacionados a ataques de programas que capturam o que é digitado no teclado, pois utilizam uma tecnologia baseada na linguagem Java, onde o usuário clica com o mouse num teclado apresentado na tela do computador, sem a necessidade de utilização do teclado convencional. Entretanto, essa solução não perdurou muito tempo como garantia de maior segurança, pois passou a ser

alvo de programas maliciosos cuja principal característica é capturar a imagem no monitor e os movimentos do mouse.

3. Riscos e vulnerabilidades dos usuários de serviços *internet banking*

O que torna os usuários da internet e seus equipamentos vulneráveis é, em especial, a curiosidade que esses têm ao aceitar e abrir, por exemplo, arquivos anexados a e-mails que recebem, que podem ser de origem conhecida ou não. Ao utilizarmos a *internet* nunca sabemos ao certo quem de fato esta do outro lado da comunicação. Com isso, pessoas mal intencionadas se aproveitam dessa possibilidade de anonimato para induzir, em geral pessoas com pouco conhecimento em informática, a instalarem programas maliciosos em seus computadores. Esses códigos maliciosos são conhecidos por *malware,* que é um termo genérico que abrange todos os tipos de programas destinados a executar ações maliciosas em um computador. São exemplos de *malwares:* **[12]**

- vírus;
- cavalos-de-tróia e backdoor;
- worms e bots;
- spyware e adware.

Os usuários de serviços de *internet banking*, por também utilizarem a internet para outras finalidades, como lazer, pesquisa, envio de mensagens e negócios são os principais alvos desses códigos maliciosos, pois suas informações bancárias são um dos principais atrativos para pessoas mal intencionadas.

3.1 Tipos de códigos maliciosos ou *malwares*

3.1.1 Vírus

Um vírus é um programa projetado e escrito para afetar um computador ao alterar a forma como ele trabalha sem o consentimento ou a permissão do responsável **[13]**. Os vírus de computador não são gerados espontaneamente. Eles precisam ser escritos e ter um objetivo específico. De maneira geral, pode-se dizer que um vírus tem duas funções distintas, a primeira é a capacidade de auto-replicação e propagação e a segunda é a de implementar o dano planejado pelo seu criador.

As principais ações de um vírus estão relacionadas a objetivos danosos, como “apagar” um disco, corromper arquivos e programas ou simplesmente desorganizar um computador. Ao contrário do que se imagina um vírus também pode ter ações benignas, o que depende da imaginação do seu criador. Como exemplo de vírus benigno, pode-se citar aqueles que são projetados para a partir de uma data ou hora predeterminada, exibir algum tipo de mensagem de texto para chamar a atenção do usuário. Porém, mesmo esse tipo de vírus pode criar problemas para o computador, pois suas ações tendem a consumir memória, causando lentidão e até eventual queda de sistema.

A disseminação de um vírus ocorre principalmente quando se inicia um aplicativo infectado, como um processador de texto ou uma planilha eletrônica, de modo que no momento em que o programa for executado, o vírus será ativado. Também é comum que o vírus se instale na memória do computador, esperando para infectar o próximo programa que for executado ou o próximo disco que for acessado. **[13]**

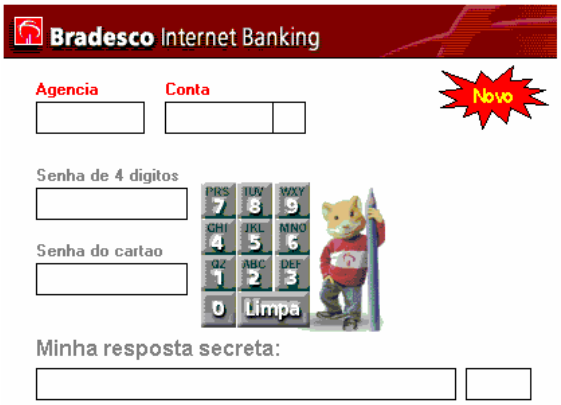
É importante frisar que não existem vírus destinados a capturar dados bancários, como número de agência, conta e senha de usuários de serviços de *internet banking*.

3.1.2 Cavalo-de-Tróia e *Backdoor*

O termo cavalo-de-tróia vem do inglês *trojan horse* e é designado para definir um programa que é normalmente recebido como um "presente". São exemplos os cartões virtuais, os álbuns de fotos, os protetores de tela ou até jogos de computador. Além de executar funções para as quais foi projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário **[12]**. O principal objetivo desses códigos é a instalação de programas do tipo *keyloggers*, usados para capturar senhas do teclado, ou *screenloggers*, usados para capturar principalmente senhas de teclados virtuais. Por isso são considerados as maiores ameaças aos usuários de serviços de *internet banking*.

Um dos cavalos-de-tróia mais famosos é o *“PWSteal.Bancos”* que tem a função de imitar, mesmo que de forma grosseira, interfaces de teclados virtuais dos principais bancos do país. Esse cavalo-de-tróia pode ser recebido por meio de arquivos anexos a e-mails. As figuras mostradas a seguir são algumas das falsas interfaces de teclado virtual utilizadas por esse trojan: **[13]**

FONTE: http://www.symantec.com/region/br/techsupp/avcenter/venc/data/br-pwsteal.bancos.html
Figura 6 – Falsa interface do teclado virtual do Banco do Brasil

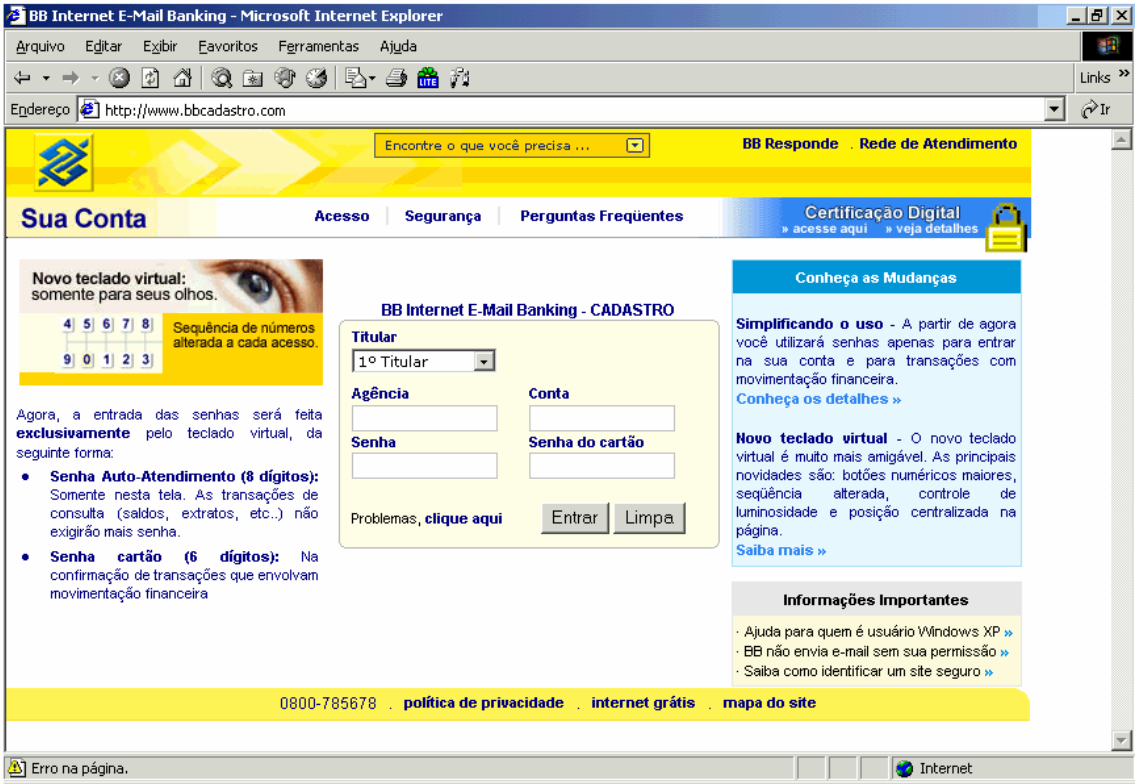


FONTE: http://www.symantec.com/region/br/techsupp/avcenter/venc/data/br-pwsteal.bancos.html
Figura 7 – Falsa interface do teclado virtual do Banco Bradesco.

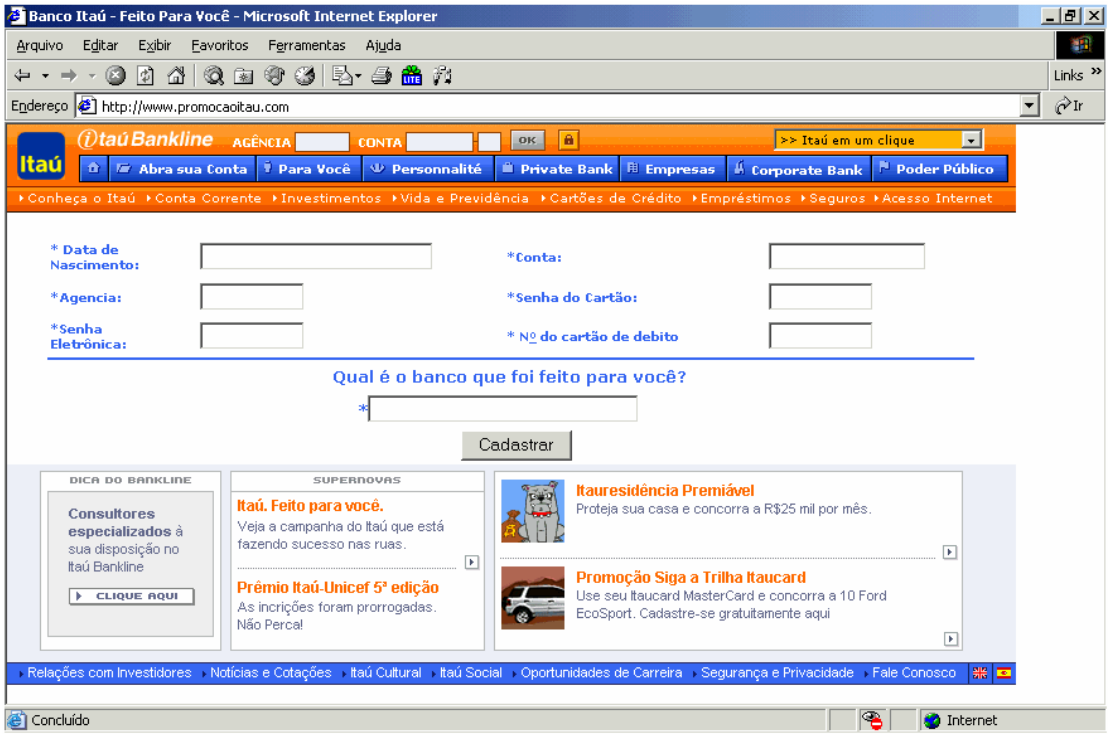
FONTE: http://www.symantec.com/region/br/techsupp/avcenter/venc/data/br-pwsteal.bancos.html
Figura 8 – Falsa interface do teclado virtual da Caixa Econômica Federal.

Esse programa, após ser instalado na máquina do usuário, passa a monitorar as janelas ativas do Internet Explorer, aguardando que seja aberta uma página da internet cujas características sejam as mesmas de determinados *sites* bancários. Desta forma, quando a página do banco é aberta, o cavalo-de-tróia exibe a tela de login falsa e, assim que as informações são postadas nessa tela, elas podem ser enviadas a um *site* FTP, controlado pelo autor do cavalo-de-tróia.

Outro método também bastante difundido é aquele que, ao invés de utilizar apenas a tela de login falsa, utiliza páginas inteiras falsificadas. Com essas páginas, quase sempre de ótima qualidade se comparadas com as originais, fica mais difícil para o cliente perceber o golpe. O usuário é normalmente induzido a acessar essas páginas por meio de *links* anexados a e-mails que recebe. Nas figuras seguintes são apresentados dois exemplos de páginas falsas.



Fonte: http://www.fraudes.org/banksites.asp?BckSt=1
Figura 9 – Página falsa do Banco do Brasil



Fonte: http://www.fraudes.org/banksites.asp?BckSt=1
Figura 10 – Página falsa do Banco Itaú

Uma diferença importante entre um cavalo-de-tróia e um vírus é que aquele não se reproduz como os vírus. Devido à segurança dos *sites* das instituições financeiras, é muito difícil que esses ambientes contenham arquivos de cavalo-de-tróia. Portanto, os alvos mais fáceis para os atacantes são sempre os usuários desses serviços e seus equipamentos. A disseminação desses programas é realizada quase sempre através de arquivos ou falsos links anexados a e-mails não solicitados, também denominados de *spams*.

Um *backdoor*, do inglês porta dos fundos, é um mecanismo introduzido no sistema de um computador com o objetivo de facilitar o acesso não autorizado a este sistema **[14]**. A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou substituição de determinado serviço por uma versão alterada, que normalmente possui recursos que possibilitam o acesso remoto por meio da internet e, podem ser inseridas por um invasor ou através de um cavalo-de-tróia. Existem pacotes de software da plataforma Windows, como o *BackOrifice* e *NetBus* que são utilizados para a administração remota e que, se mal configurados ou utilizados sem a permissão do usuário, podem ser classificados com *backdoors.* **[12]**

A principal diferença entre um cavalo-de-tróia e um *backdoor* é que este não tem uma carga destrutiva ou maléfica por padrão e geralmente permite o acesso remoto ao computador infectado. Já a principal semelhança é que nenhuma dessas duas categorias infecta arquivos. Isto significa que não há opções como "desinfectar" ou "reparar" estes arquivos, porque não há nada para ser desinfectado ou reparado. **[15]**

3.1.3 *Worms* e *Bots*

Os *worms*, do inglês vermes, são programas maliciosos que se reproduzem de um sistema para outro automaticamente, ou seja, sem usar um arquivo hospedeiro para infectarem e se espalharem a partir dele, como ocorre com os vírus **[13]**. O grande perigo dos *worms* é a sua capacidade de se replicar em grande quantidade. Eles podem enviar cópias de si mesmo a todas as pessoas que constam no catálogo de endereços de e-mail da máquina infectada, com isso, os computadores dessas pessoas passam a fazer o mesmo, causando um efeito dominó de alto tráfego de rede que pode torná-las mais lentas.

O *bot* é um programa capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador. O que o diferencia do *worm* é que ele dispõe de mecanismos de comunicação com o invasor, permitindo que o *bot* seja controlado remotamente. A comunicação normalmente é feita por meio de um servidor de IRC (*Internet Relay Chat*). O *bot* aguarda as instruções do invasor, que monitora as mensagens que estão sendo enviadas para esse canal. **[12]**

3.1.4 Spyware e Adware

Spywares são programas que têm como objetivo espionar as atividades dos internautas ou capturar informações sobre eles. Para contaminar um computador, os *spywares* podem vir embutidos em softwares desconhecidos ou serem baixados automaticamente quando o internauta visita *sites* de conteúdo duvidoso. Já o *adware* é um

tipo de software desenvolvido para apresentar propagandas, seja através de um *browser*, seja através de algum outro programa instalado em um computador.

Tanto os *spywares* quanto os *adwares* podem ser utilizados de forma legítima, porém, na maioria das vezes são utilizados de forma não autorizada e maliciosa. A seguir são apresentadas algumas funcionalidades implementadas por *spywares* que podem ter relação com o uso legítimo ou malicioso: **[12]**

- alteração da página inicial apresentada no browser do usuário;
- varredura dos arquivos armazenados no disco rígido do computador;
- captura de senhas bancárias e números de cartões de crédito;
- captura de outras senhas usadas em *sites* de comércio eletrônico.

Na maioria das vezes, os *spywares* são utilizados com intenção maliciosa. Assim que instalado, ele passa a monitorar todos os acessos a *sites* enquanto o usuário navega na *internet*. Desta maneira, sempre que o usuário acessar determinados *sites* bancários ou de comércio eletrônico, um *keylogger* ou um *screenlogger* será ativado para capturar os dados informados.

3.2 Formas de proteção

Para se proteger dos chamados *malwares*, o usuário tem à disposição uma grande variedade de softwares de segurança, que podem ser gratuitos ou não. A opção depende, obviamente, do que se quer proteger. Os softwares pagos, normalmente oferecem mais recursos e a possibilidade de atualizações periódicas, por um período determinado e sem a cobrança de valores adicionais. Já os softwares do tipo *freeware* ou gratuito, apesar de oferecer menos recursos, se mostram bastante eficientes se o usuário souber como utilizá-lo e procurar regularmente fazer as atualizações necessárias, pois alguns desses programas, a exemplo daqueles que são pagos, também permitem que o usuário faça atualizações por meio da internet.

Porém, utilizar softwares de antivírus, anti-spyware e anti-trojan não garante uma proteção eficaz ao usuário de serviços de *internet banking*. Também é necessário que

este não deixe de atualizar periodicamente seu sistema operacional, pois regularmente os fabricantes desses softwares disponibilizam correções para falhas de segurança.

Mesmo sabendo que nenhum sistema é totalmente imune a ataques, é possível dificultá-los, diminuindo assim as chances de sucesso de uma pessoa mal intencionada e aumentando a possibilidade de um usuário, principalmente de serviços de *internet banking*, não sofrer um ataque a seu sistema e, fundamentalmente a sua conta bancária.

A proposta que será apresentada nos próximos capítulos tem como objetivo mostrar uma alternativa para tornar bem mais difícil os ataques contra os usuários de serviços bancários pela *internet*, pois agrega na forma de autenticação dos bancos não só um conhecimento que o usuário sabe, mas também algo que ele tem, que é um *smart card* com um certificado digital.

4. Certificados Digitais ICP Brasil

4.1 A ICP Brasil

A Infra-estrutura de Chaves Públicas Brasileira (ICP Brasil) foi instituída com a publicação da Medida Provisória 2.200-2, de 24.10.2001, e visa garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. É composta por representantes de entidades prestadoras de serviços ordenadas em conformidade com as diretrizes e normas técnicas estabelecidas por um Comitê Gestor (CG), vinculado à Casa Civil da Presidência da República e que tem como função determinar as políticas a serem executadas pela Autoridade Certificadora Raiz. **[16]**

Além do Comitê Gestor, integra a estrutura da ICP Brasil, uma Autoridade Certificadora Raiz (AC-Raiz), Autoridades Certificadoras (ACs) e as Autoridades de Registro (ARs). O papel de AC-Raiz é exercido pelo Instituto Nacional de Tecnologia da Informação (ITI) que é responsável pela execução das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor. Também realiza o credenciamento e auditoria das ACs e das ARs. Além do ITI, estão credenciadas atualmente junto a ICP Brasil as Autoridades Certificadoras da Secretaria da Receita Federal (SRF), Serpro, Certisign, Serasa, Caixa Econômica Federal (CEF), Poder Judiciário (AC-Jus), Sindicato dos Corretores do Estado de São Paulo (AC-Sincor) e Presidência da República (PR). **[17]**

As ACs são entidades públicas ou pessoas jurídicas de direito privado credenciadas à AC-Raiz e responsáveis, entre outras atividades, pela emissão, gerenciamento e revogação de certificados digitais. Vinculadas as Autoridades Certificadoras estão as ARs, responsáveis pela identificação presencial e validação dos documentos dos interessados em adquirir certificados. Na **figura 11**, são mostradas algumas das principais Autoridades de Registro e suas respectivas Autoridades Certificadoras na hierarquia da ICP Brasil.

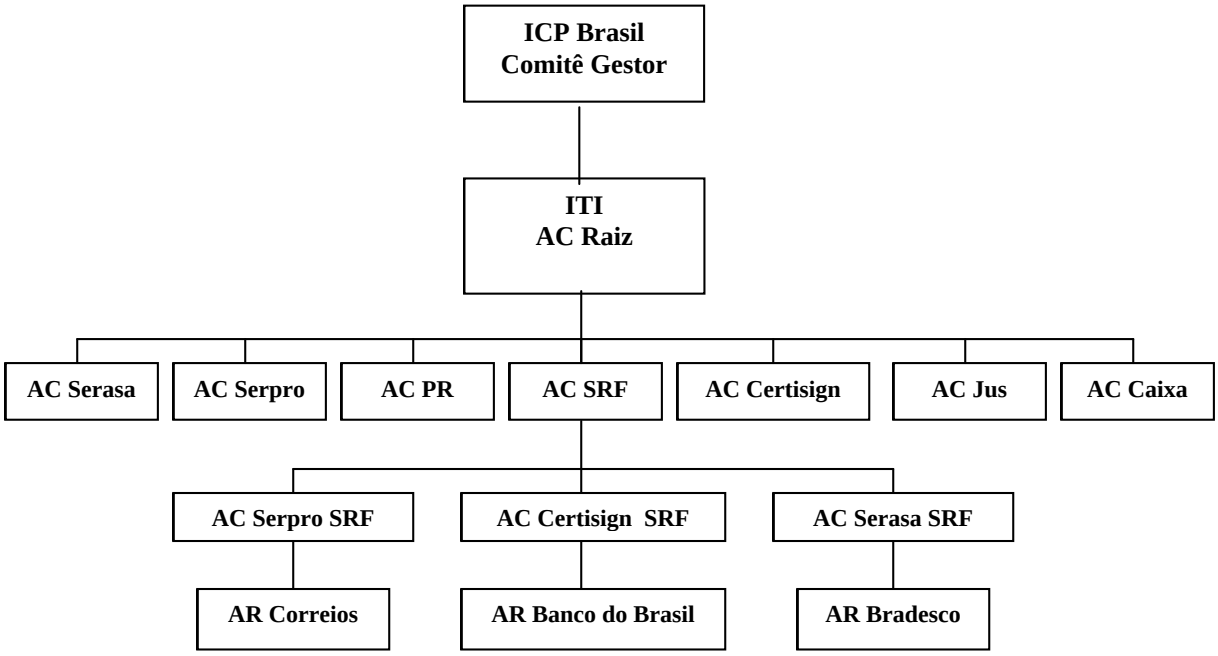


Figura 11 – Infra-estrutura da ICP Brasil e suas principais entidades

4.2 Obrigações da Terceira Parte

De acordo com a Resolução nº 7 do Comitê Gestor da ICP Brasil, considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital. No caso deste trabalho, terceira parte será a instituição financeira que aceitar o uso de certificados digitais por parte de seus clientes em suas aplicações.

Constituem direitos da terceira parte:

- Recusar a utilização do certificado para fins diversos dos previstos na Política de Certificação correspondente;
- Verificar a qualquer tempo, a validade do certificado. Um certificado emitido por AC integrante da ICP Brasil é considerado válido quando:

  - não constar na Lista de Certificados Revogados (LCR) da AC emitente;
  - não estiver expirado;
  - puder ser verificado com o uso de certificado válido da AC emitente.

4.3 Tipos de Certificados Digitais na ICP Brasil

O certificado digital é um documento eletrônico utilizado para identificar uma pessoa, física ou jurídica, em transações virtuais. É assinado digitalmente por uma AC e contém dados sobre o emissor e o seu titular. A função do certificado digital é a de vincular uma pessoa ou uma entidade a uma chave pública.

Somente as transações realizadas com processo de certificação envolvendo certificados emitidos por autoridades credenciadas junto à ICP Brasil presumem-se verdadeiras em relação aos signatários, sem a necessidade de pré-acordo entre as partes, dando validade jurídica aos documentos assinados digitalmente.**[16]**

Na Infra-estrutura de Chaves Públicas Brasileira (ICP Brasil), estão previstos 8 tipos de certificados digitais destinados para usuários finais, sendo que 4 estão relacionados com assinatura digital (A1, A2, A3 e A4) e quatro com sigilo (S1, S2, S3 e S4).

Os certificados de assinatura (A) são utilizados na confirmação de identidade na WEB, correio eletrônico, redes privadas virtuais e assinatura de documentos eletrônicos com verificação da integridade de suas informações. Já os certificados de sigilo (S) são utilizados na cifragem de documentos, em base de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir seu sigilo.

Os tipos de A1 a A4 e de S1 a S4 definem escalas de requisitos de segurança nas quais os tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos. **[18]**

Tipo de Certificado	**Chave Criptográfica**			**Validade Máxima do Certificado (anos)**
	Tamanho (bits)	**Processo de Geração**	**Mídia Armazenadora**	
A1 e S1	1024	*Software*	Cartão Inteligente ou *Token*, ambos sem capacidade de geração de chave e protegidos por senha.	1
A2 e S2	1024	*Hardware*	Cartão Inteligente ou *Token*, ambos sem capacidade de geração de chave e protegidos por senha.	2
A3 e S3	1024	*Hardware*	Cartão Inteligente ou *Token*, ambos com capacidade de geração de chave e protegidos por senha, ou *hardware* criptográfico aprovado pelo CG da ICP Brasil	3
A4 e S4	2048	*Hardware*	Cartão Inteligente ou *Token*, ambos com capacidade de geração de chave e protegidos por senha, ou *hardware* criptográfico aprovado pelo CG da ICP Brasil	3

Tabela 1 – Tipos de Certificados ICP Brasil

4.4 O padrão X.509

O padrão X.509 define um formato padrão para certificados digitais. Sua primeira versão foi publicada em 1988 como parte das recomendações da União Internacional de Telecomunicações ITU-T, para o padrão de diretório X.500. Um diretório pode ser definido como uma base de dados on-line que contém várias informações. **[19]**

Desde quando surgiu, o padrão X.509 já foi revisado duas vezes, sendo a primeira em 1993, onde foram acrescentados ao formato X.509 os campos identificador do emitente e identificador do proprietário, que passou assim à versão v2. A segunda revisão, versão v3, foi completada em 1996 e acrescentou aos certificados os chamados campos de extensão, que abrangem as informações sobre a política, a chave, os atributos de sujeito e de emissor e as restrições do caminho de certificação.

Todos os certificados X.509v3 têm os seguintes campos:

- **Versão:** diferencia as sucessivas versões do certificado, como Versão 1, Versão 2 e Versão 3.
- **Número Serial do Certificado:** contém um número inteiro que é um identificador único de cada certificado e é gerado pela Autoridade Certificadora.
- **Algoritmo de assinatura:** indica o identificador do algoritmo utilizado para assinar o certificado.
- **AC Emitente**: identifica o nome da Autoridade Certificadora que emitiu o certificado.
- **Período de validade:** identifica o período de tempo em que o certificado deve ser considerado válido, a menos que ele seja revogado por outra circunstância diferente do tempo.
- **Nome do proprietário**: identifica o nome do dono do certificado. Esse campo não deve ser nulo.
- **Algoritmo de identificação da chave pública:** contém a chave pública e a identificação do algoritmo utilizado.
- **Identificador do emitente:** contém o identificador único da Autoridade Certificadora que emitiu o certificado. É um campo opcional que pode ser utilizado apenas nas versões 2 e 3 do padrão X.509.

- **Identificador do proprietário:** contém o identificador único do dono do certificado. É um campo opcional que pode ser utilizado apenas nas versões 2 e 3 do padrão X.509.
- **Extensões:** permitem que uma AC acrescente informações que normalmente não seriam fornecidas pelo conteúdo básico de um certificado.
- **Assinatura Digital da AC:** identificador do algoritmo utilizado e a assinatura digital da AC que emitiu o certificado.

Atualmente, os certificados utilizados na ICP Brasil seguem o padrão X.509, mais especificamente a versão 3, conforme estabelecido na Resolução nº 1 do Comitê Gestor da ICP Brasil. Por isso, com exceção dos campos opcionais, todos os demais campos mostrados na **figura 12** devem constar nos certificados ICP Brasil, em particular nos certificados do tipo A3, objeto deste trabalho.

Figura 12 – Estrutura do certificado X.509 v3

4.5 Características do certificado

4.5.1 Criptografia Assimétrica

A segurança dos certificados digitais baseia-se na técnica de criptografia assimétrica, também conhecida por criptografia de chaves públicas, que é um método que utiliza um par de chaves, uma em cada extremidade do processo, sendo uma pública e outra privada. A chave pública pode ser distribuída livremente, enquanto que a chave privada é de conhecimento apenas de seu titular. O principal algoritmo usado na criptografia assimétrica é o RSA, cujas chaves para certificados ICP Brasil dos tipos A1 a A3 são de 1024 bits. **[18]**

No caso de mensagens cifradas com a chave pública, somente a correspondente chave privada pode ser utilizada para decifrá-la. Do mesmo modo uma mensagem cifrada com a chave privada pode somente ser decifrada pela sua chave pública correspondente.

Os algoritmos de chave pública podem ser utilizados para garantir a autenticidade, a confidencialidade e o não-repúdio em uma transação. A confidencialidade é garantida quando se utiliza a chave pública para cifrar mensagens, com isso apenas o titular da chave privada pode decifrá-la. Para garantir a autenticidade, a chave privada é que deve ser utilizada para cifrar a mensagem, desta forma garante-se que apenas o titular da chave privada poderia ter cifrado a mensagem que, por sua vez, pode ser decifrada com a correspondente chave pública. **[1]**

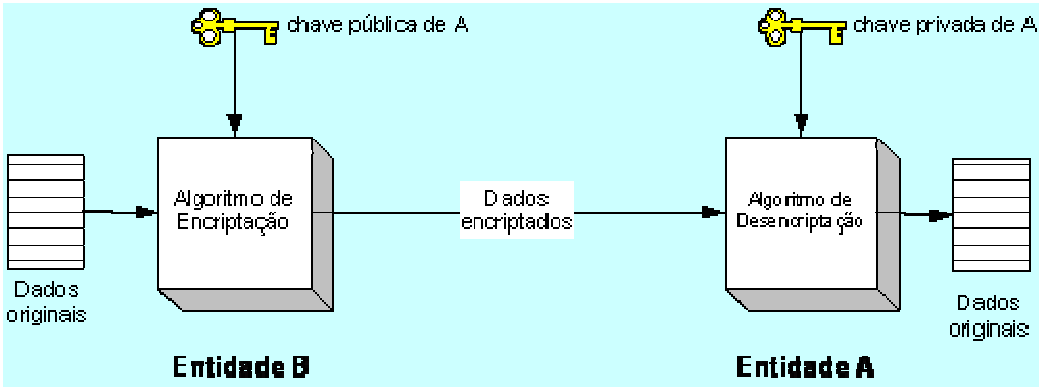


Figura 13 - Criptografia Assimétrica utilizada para garantir a confidencialidade

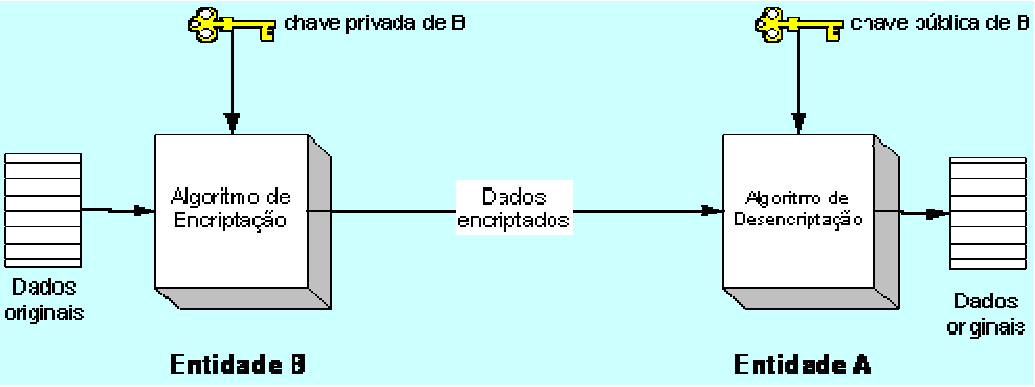


Figura 14 - Criptografia Assimétrica utilizada para garantir a autenticidade

A criptografia assimétrica acaba com o problema da distribuição de chaves, comum na criptografia simétrica, que utiliza a mesma chave para cifrar e decifrar uma mensagem. Com a utilização da chave pública, não há a necessidade do compartilhamento de uma mesma chave nem de um pré-acordo entre as partes interessadas na comunicação.

4.5.2 Assinatura Digital

A principal finalidade dos certificados digitais de assinatura, dos tipos A1 a A4, é comprovar a identidade de um indivíduo na rede através do processo de assinatura digital. Ao contrário da assinatura manuscrita, a assinatura digital é praticamente impossível de ser falsificada, em decorrência das técnicas matemáticas utilizadas e da criptografia assimétrica. **[19]**

A base da assinatura digital está no par de chaves pública e privada. A chave pública envolvida em um processo de assinatura digital deve ser conhecida pela entidade que vier a receber “algo” assinado para que possa realizar a devida validação.

Com a assinatura digital também é possível verificar a integridade de uma mensagem, ou seja, se esta não sofreu nenhuma alteração durante a transmissão. Isto é realizado por meio da aplicação de uma função matemática denominada *hash*, que gera um valor pequeno, de tamanho fixo e único para cada texto, chamado de valor *hash* e derivado da mensagem que se pretende assinar, que pode ser de qualquer tamanho **[20]**. Após o valor *hash* de uma mensagem ser calculado, qualquer modificação em seu

conteúdo, por menor que seja, irá gerar um novo valor *hash*, indicando que a mensagem perdeu a integridade.

O algoritmo de *hash* utilizado nos certificados digitais do tipo A3 é o *Secure Hash Algorithm*, mais conhecido por SHA-1 **[18]**. Assim que uma mensagem de qualquer tamanho é submetida a esse algoritmo, ele gera uma saída de 160 bits chamada de resumo da mensagem. Esse resumo pode ser incorporado à mensagem original e transmitido ao destinatário. Este, para verificar a integridade da mensagem precisa reaplicar a função *hash* e comparar com o que recebeu e, caso os valores sejam iguais, pode-se garantir que a mensagem não sofreu alteração.

Figura 15 – Assinatura digital utilizando criptografia assimétrica

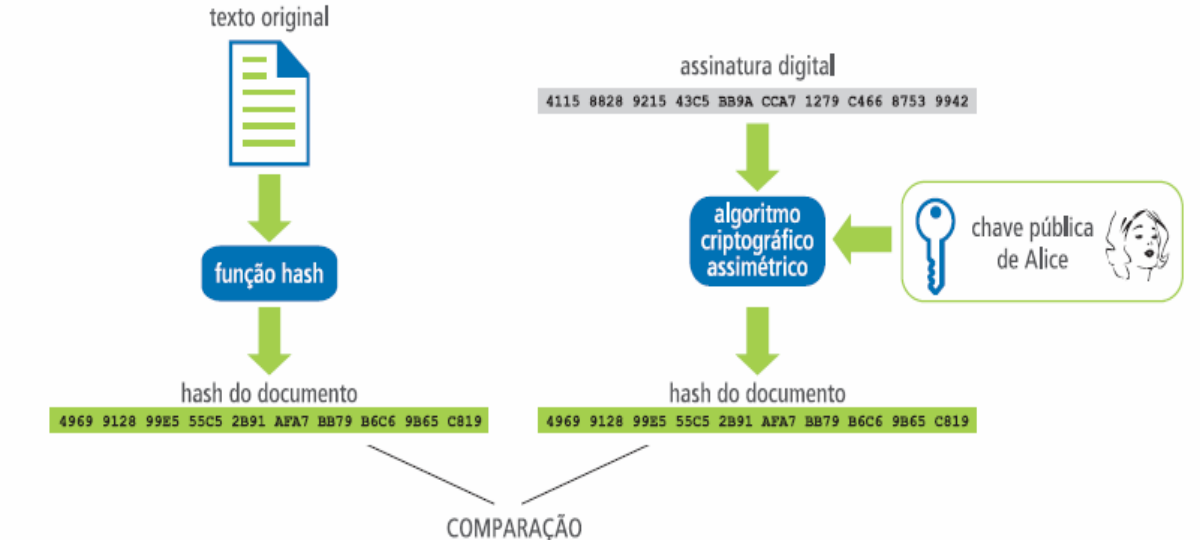


Figura 16 – Conferência da Assinatura Digital

5. Processo de Emissão de Certificados Digitais ICP Brasil

Um dos fatores que mais agrega confiabilidade aos certificados ICP Brasil, é o rigoroso processo exigido para aquisição desses certificados. Conforme determina a legislação que regulamenta o uso desses certificados **[21]**, para adquirir qualquer um dos tipos mencionados no **item 4.3**, é necessário que o interessado realize um pré-cadastro junto a uma das Autoridades de Registro (AR) credenciadas e, posteriormente compareça a uma Autoridade de Registro (AR), vinculada à AC onde foi realizado o pré-cadastro, portando uma foto 3x4 recente e, no mínimo os seguintes documentos acompanhados de cópia, conforme determina a Resolução nº 31 do Comitê Gestor da ICP Brasil:

- Cédula de Identidade ou Passaporte, se estrangeiro;
- Cadastro de Pessoa Física;
- Comprovante de Residência;
- PIS, PASEP, se aplicável;
- Título de Eleitor, se aplicável;
- Mais um documento oficial com fotografia, no caso de certificados de tipos A4 e S4; e
- Os documentos acima relacionados do responsável, caso o solicitante seja incapaz.

Na Autoridade de Registro, o pedido deve ser aprovado por dois funcionários, denominados Agentes de Registro ou Agentes de Validação. O primeiro agente realiza a etapa de validação do pedido com base nos documentos apresentados pelo solicitante. Já o segundo agente, realiza a confirmação da validação, com base nos dados validados para, posteriormente, solicitar à Autoridade Certificadora a emissão do certificado.

Os Agentes de Validação, para realizarem suas atividades, recebem treinamento específico para tal, que inclui curso de grafoscopia, necessário para permitir o reconhecimento de assinaturas autógrafas, e de segurança da informação. Estes também devem apresentar atestado de idoneidade financeira, de empregos anteriores e certidão negativa de antecedentes criminais. Além disso, todas a atividades das Autoridades

Certificadoras e das Autoridades de Registro da ICP Brasil, estão sujeitas a processos anuais de auditoria por parte do Instituto Nacional de Tecnologia da Informação (ITI) e das próprias Autoridades Certificadoras, no caso das Autoridades de Registro.

A **figura 17** ilustra as etapas necessárias para aquisição de um certificado digital emitido no âmbito da ICP Brasil.

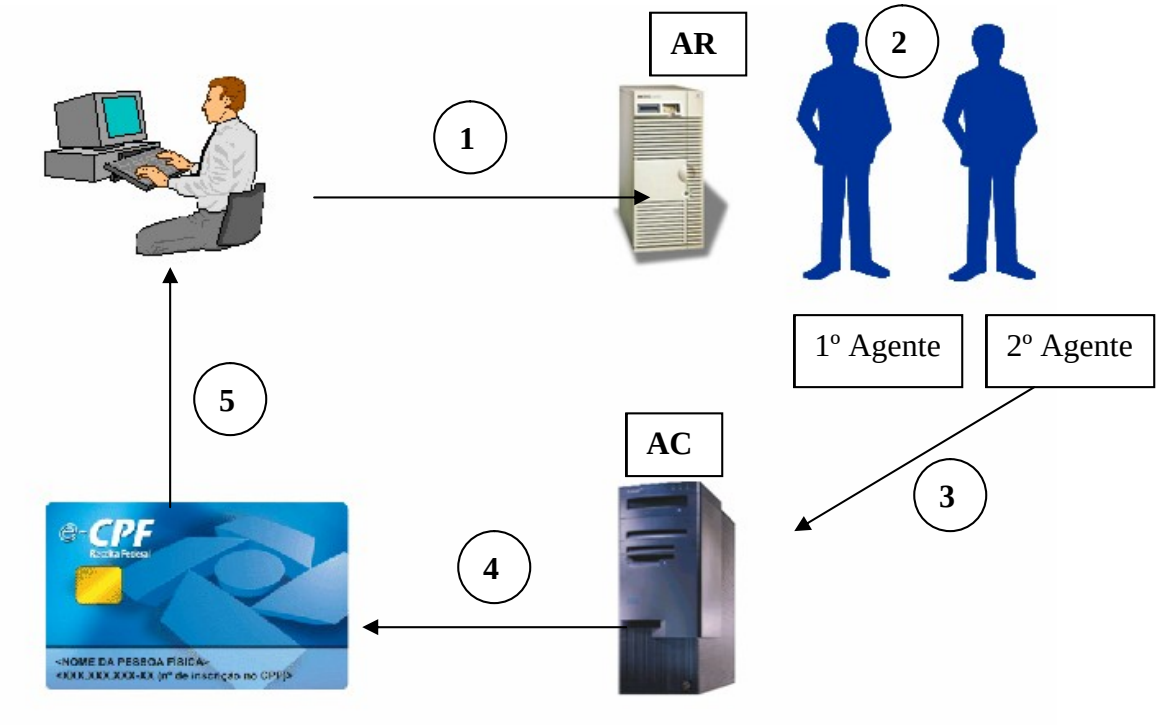


Figura 17 – Etapas para aquisição de um Certificado Digital ICP Brasil

Os números de 1 a 5 representam, respectivamente:

- **Etapa 1:** o interessado realiza via internet (de qualquer lugar), pré-cadastro em *site* específico da Autoridade de Registro, onde solicita o certificado. Após realizar o pré-cadastro, deve comparecer fisicamente na Autoridade de Registro e apresentar os documentos necessários ao primeiro agente de validação.
- **Etapa 2:** o primeiro agente, valida o pedido do interessado, com base nos documentos apresentados.
- **Etapa 3:** o segundo agente confirma a validação do pedido e encaminha, via internet, o pedido para a Autoridade Certificadora, solicitando a emissão do certificado.

- **Etapa 4:** após as etapas de validação e confirmação da validação do pedido, a AC emite o certificado digital.
- **Etapa 5:** o certificado digital e o par de chaves criptográficas são gerados e recebidos pelo titular.

Todas as atividades realizadas pelas entidades que pertencem à ICP Brasil estão amparadas atualmente por 45 Resoluções aprovadas pelo Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira e podem ser consultadas no *site* do Instituto Nacional de Tecnologia da Informação - ITI **[21]**. Além das resoluções mencionadas, existem outros documentos importantes, entre eles estão:

- **Declaração de Práticas de Certificação (DPC):** expõe as regras operacionais das atividades de determinada AC e também os procedimentos gerais para identificação dos usuários dos certificados digitais e a obrigação das partes envolvidas, entre outras informações. Este documento é único para cada AC.

- **Políticas de Certificado (PC):** contém detalhes específicos sobre determinado tipo de certificado, como as informações que ele contém e o tamanho das chaves criptográficas associadas. Ao contrário da DPC, existe uma PC para cada tipo de certificado emitido por uma Autoridade Certificadora.

6. O uso de Certificados Digitais ICP Brasil no país

Existem atualmente no Brasil, principalmente entre as entidades governamentais, várias aplicações destinadas ao uso de certificados digitais ICP Brasil, entre elas:

- A **Presidência da República** e os **Ministérios** utilizam certificados digitais da ICP Brasil para tramitação eletrônica de documentos oficiais, inclusive os que serão publicados no Diário Oficial da União;
- No **Estado de Pernambuco**, lançamentos de registros de operações e prestações relativas ao ICMS passaram a ser obrigatoriamente efetivados por meio de arquivo eletrônico assinado digitalmente com uso de certificado digital;
- A **Secretaria da Receita Federal** mantém em sua página na Internet, o Centro Virtual de Atendimento ao Contribuinte, e-CAC, que disponibiliza aos portadores de certificados digitais e-CPF e e-CNPJ, acesso a serviços que sem a tecnologia, só poderiam ser realizados presencialmente em seus postos;
- A **Imprensa Oficial do Estado de São Paulo** implantou a certificação digital de ponta a ponta em seu sistema que automatiza o ciclo de publicações na Internet;
- A **Superintendência de Seguros Privados SUSEP** publicou, em novembro/2004, a circular 277 que regulamenta o uso da certificação digital no mercado de seguros. Os documentos eletrônicos relativos às operações de seguros, de capitalização e de previdência complementar aberta poderão ser assinados digitalmente com certificados digitais;
- O **Banco Central do Brasil**, através da Circular 3234 de maio/2004, regulamentou o uso de certificados digitais ICP Brasil para assinatura de contratos de câmbio.

7. Dispositivos de armazenamento e portabilidade de certificados digitais

7.1 *Smart Cards*

Smart cards são cartões especiais que possuem processadores embutidos. São projetados de forma que tenham capacidade de processamento específica para a função que estão realizando. Atualmente existem dois tipos, cartões de memória e de microprocessador. Os cartões de memória, não realizam nenhum tipo de processamento, pois toda a lógica do sistema esta contida nas leitoras. Esses são utilizados para armazenar informações e, dependendo da tecnologia aplicada, podem ser descartáveis ou reutilizáveis. Já os cartões de microprocessador, utilizados neste trabalho, são aqueles que realmente podem ser chamados de *smart* ou inteligentes, pois possuem Unidade Central de Processamento (CPU) com capacidade para executar comandos, além de possuir áreas de memória para armazenar informações **[22]**.

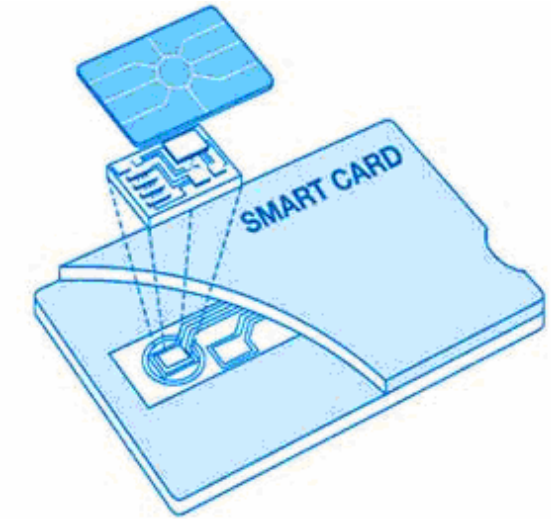


Figura 18 – Smart card com CPU

O chip dos cartões com CPU é capaz de gerenciar os dados, organizados em estruturas de arquivos, via um “sistema operacional de cartão”, também conhecido por COS, do inglês *card operating system*. Ao contrário de outros sistemas operacionais, esse software controla acesso à memória do usuário no cartão. O resultado disso é que várias funções e aplicativos podem residir no cartão **[20]**. Esses cartões possuem espaço

suficiente para armazenar certificados digitais, a maior parte deles, até três certificados do tipo A3.

Embora existam muitos tipos de *smart cards*, qualquer um pode ser classificado quanto à forma de conexão com a leitora que pode ser por contato físico ou sem contato físico. Por contato físico entende-se a inserção do cartão na leitora, onde os contatos dos terminais do cartão com os da leitura, permitem a troca de dados entre ambos. É importante salientar que todos os *smart cards* possuem terminais para este tipo de conexão.

A segunda classe se refere aos cartões que não necessitam de contato físico com a leitora, o que indica que a conexão é feita através de ondas eletromagnéticas. A ausência do ato de inserção traz benefícios como economia de tempo e não desgaste dos terminais do cartão.

Neste trabalho será utilizado um cartão por contato físico.

7.1.1 Vantagens dos smart cards

O uso de smart cards traz inúmeras vantagens, entre as quais vale destacar:

- **Confiabilidade:** os cartões devem atender as especificações da ISO (*International Standards Organization*) e passar por uma bateria de testes que abrangem: testes de torção, de flexibilidade, de desgaste, de concentração de carga, temperatura, umidade, eletricidade estática, ataque químico, ultra-violeta, raio X e testes de campo magnético.
- **Correção de erro:** o Sistema Operacional do Chip (COS) realiza seu próprio algoritmo de correção de erro.
- **Capacidade de armazenamento:** a memória mais utilizada nos *smart cards* são as EEPROM (*Electrically Erasable Programmable Read-Only Memory*) que possuem capacidade de 8K - 128K bit. Entretanto, com as modernas técnicas de compressão, a quantidade de informação armazenada em um *smart card* pode ser significativamente expandida.

- **Segurança:** *smart cards* são muito seguros. As informações armazenadas no chip são difíceis de serem copiadas ou alteradas, ao contrário dos cartões de tarja magnética que podem ser facilmente clonados. O microprocessador e o co-processador do chip suportam criptografia, autenticação e assinatura digital.
- **Capacidade de processamento:** cartões mais antigos usavam um micro-controlador de 8-bits com clock de 16 MHz. Os cartões mais modernos utilizam um micro-controlador RISC de 32-bits rodando a um clock de 25 a 32 MHz, com um co-processador para a criptografia.

Como a demanda por criptografia vem crescendo, tem se exigido também cada vez mais poder de processamento da CPU dos cartões. Um processo de decriptação RSA 1024 bits, por exemplo, pode demorar até 10 segundos. Diante disto, alguns fabricantes inserem co-processadores no cartão, a fim de acelerar esse serviço.

A comunicação entre o cartão e o software de aplicação é do tipo mestre (software) e escravo (cartão). O software envia comandos ao cartão e espera por uma resposta. O cartão nunca envia dados ao software exceto em resposta a um comando.

Os sistemas operacionais dos *smart cards* suportam dois tipos de transferência: por caractere ou por bloco. A transferência por caractere ocorre quando os dados são transferidos caractere a caractere até formar uma palavra. Já na transferência por bloco, são transmitidos quadros inteiros por vez, o que faz deste tipo de transferência mais complexo que o outro.

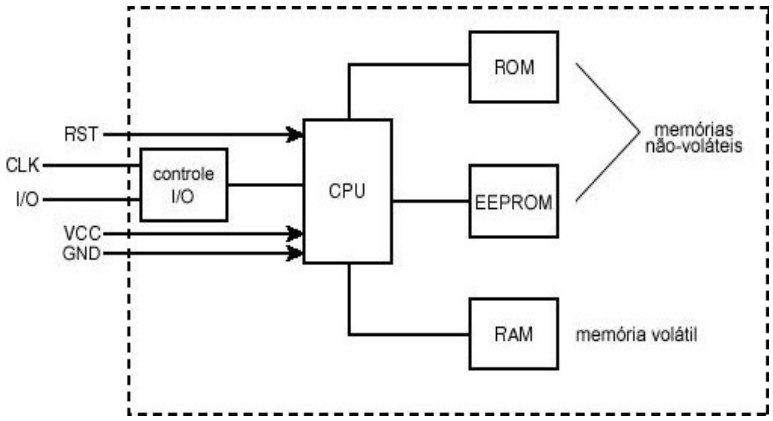


Figura 19 - Elementos de um smart card

7.1.2 Leitoras de *smart cards*

Como o cartão utilizado neste trabalho é do tipo por contato físico, será necessário utilizar também uma leitora de *smart card* para que o mesmo possa ser lido. Na **figura 20** são mostrados dois modelos de leitoras atualmente utilizados para operacionalizar *smart cards* que armazenam certificados digitais.

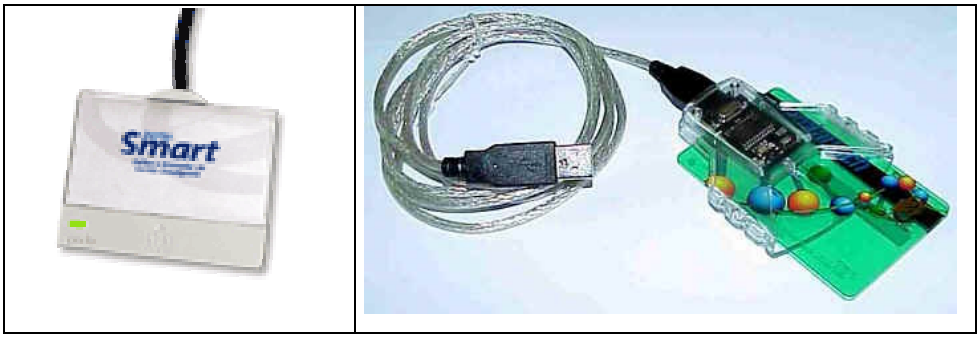


Figura 20 – Leitoras de smart cards (marcas Perto e Gemplus respectivamente)

As leitoras são capazes de ler e gravar em cartões inteligentes. Podem ter interface para a porta serial, Universal Serial Bus (USB), slots de PCMCIA e para leitoras de teclado. Neste trabalho será utilizada uma leitora para interface USB, da marca Gemplus, similar a mostrada na **figura 20**.

Uma informação importante é que as leitoras, para funcionarem necessitam da instalação de um driver específico que é fornecido pelo fabricante.

7.2 Tokens

Existem no mercado vários fabricantes de *tokens*, entretanto os mais conhecidos para os serviços de *internet banking*, com mais de 90% do mercado, são os da empresa Vasco **[19]**. Para *internet banking*, as soluções de segurança envolvem tecnologia relacionada ao uso de *tokens* com as chamadas senhas dinâmicas, que são àquelas que mudam a cada minuto. Desta maneira, somente os titulares desses dispositivos, com suas senhas particulares, têm acesso às informações de suas contas, evitando o roubo de identidades de forma simples, prática e intuitiva. É uma solução que já existe em mais de 200 bancos em todo o mundo, e sua instalação e utilização pode ser bastante simples,

dependendo obviamente do conhecimento de informática do usuário **[19]**. Atualmente, as soluções de *tokens* USB também permitem armazenar nestes dispositivos, certificados digitais ICP Brasil do tipo A3, o mesmo apresentado neste trabalho.

7.2.1 Tokens USB

O *token* USB, bem como o *smart card*, é um hardware criptográfico utilizado para armazenar, dependendo da sua capacidade, um ou mais certificados digitais e suas respectivas chaves criptográficas, chave pública e chave privada. Os tokens USB agregam em um único dispositivo as funções de leitora e de *smart card*.

A exemplo de uma leitora de smart card, um token também necessita para o seu correto funcionamento, da instalação de um software para permitir o reconhecimento deste dispositivo pela máquina em que o mesmo será utilizado.

Figura 21 – Tokens USB

7.3 Diferenças entre *tokens* e *smart cards*

Apesar de ambos terem como uma de suas finalidades principais o armazenamento de certificados digitais, estes dispositivos apresentam algumas diferenças que são importantes destacar. A primeira está no formato físico. Um *smart card* é idêntico a um cartão de crédito e pode conter o nome de seu titular, foto e outras informações como o nome da empresa ou da instituição. Já um *token* não possui essas informações, tem no máximo o logotipo do fabricante ou da empresa responsável pela emissão do certificado digital. O tamanho do *token* é semelhante ao de uma chave doméstica e pode ser facilmente carregado em um chaveiro.

Outra diferença importante está na facilidade de uso e portabilidade de cada dispositivo. Enquanto que o cartão necessita de uma leitora USB ou Serial para ser utilizado, além da instalação de um driver da leitora e de um software para gerenciar o uso do cartão, o *token* USB precisa apenas da instalação do software de gerenciamento do mesmo, além de um computador que tenha uma porta USB disponível.

A decisão quanto a qual deles utilizar deve ser avaliada principalmente pela funcionalidade. Caso se pretenda utilizar o certificado digital com o objetivo de associá-lo à identificação física, como nos casos de controle de acesso físico, os cartões são mais apropriados pelo fato de se poder agregar uma foto e o nome do usuário.

De modo geral, ambientes mais corporativos e controlados preferem *tokens* e ambientes abertos adotam cartões. Entende-se que nas empresas os *tokens* se mostram mais eficientes, pois trata-se de apenas um único dispositivo, contra dois na opção *smart card* e leitora. Já no universo de varejo, cartões são mais conhecidos, por já estarem enraizados na cultura de uso de transações eletrônicas .

Na hora da escolha é importante destacar que o desempenho também é um fator importante, que pesa a favor dos *tokens* na razão de sete para um, pois o processamento criptográfico dentro deles é, em média, sete vezes mais rápido do que em *smart cards*, devido à forma de comunicação de dados. Nos cartões, a chave privada deve ser lida primeiro pela leitora, que só depois transmite a informação para o computador. No *token*, essa intermediação não existe, e está limitada apenas à velocidade da porta USB. **[23]**.

8. Solução proposta

Foi desenvolvida uma interface de autenticação web que representa o site de um banco qualquer, denominado neste trabalho de “Banco Local”, para simular o acesso de um usuário de certificado digital ICP Brasil do tipo A3 ao serviço de *internet banking* deste banco. Para isso foram utilizadas as linguagens de programação Java para o desenvolvimento da applet e HTML para a construção das páginas web.

Na proposta apresentada, o usuário será autenticado no *site* da instituição financeira ao informar corretamente para a aplicação os seguintes dados:

- prefixo da agência;
- número da conta-corrente;
- PIN (personal identication number) do smart card.

A aplicação irá verificar a autenticidade, a validade do certificado e se o mesmo está vinculado à agência e conta-corrente informada.

A simulação será feita mediante a utilização de um computador e de um usuário que irá interagir com este, como se estivesse acessando sua conta-corrente pela internet, em sua casa ou local de trabalho. Também serão mostradas tentativas de acesso não autorizadas. Isto será mostrado quando o usuário tentar utilizar um certificado vencido, revogado ou que não esteja cadastrado e vinculado a determinada agência e conta-corrente.

Como pré-requisito para o funcionamento da aplicação, será necessário que o cliente já possua um *smart card*, uma leitora de *smart card* instalada em seu computador e um certificado digital ICP Brasil do tipo A3 previamente vinculado a uma determinada agência e conta-corrente.

8.1 Requisitos funcionais da aplicação

Mostrar como a utilização da solução pelas instituições financeiras que resolverem adotá-la pode trazer vantagens de segurança, obtidas com os Certificados Digitais no padrão proposto.

Com relação a simulação, o resultado esperado é que, caso o usuário não seja validado, a aplicação seja capaz de identificar e tratar as tentativas de acesso não autorizadas, retornando como resposta mensagens do tipo:

a) “Verifique se o cartão encontra-se na leitora ou se a senha confere”;
b) “Certificado não pertence à agência/conta informada”;
c) “Certificado vencido”;
d) “Certificado revogado”.

Caso o usuário seja validado, o sistema deverá apresentar uma mensagem informando que o acesso foi liberado, do tipo: “ACESSO LIBERADO”.

8.2 O certificado e o *smart card* escolhidos para o trabalho

Neste trabalho optou-se por utilizar um certificado digital padrão A3, do tipo e-CPF, armazenado em *smart card*. A escolha desse certificado deveu-se ao fato da Federação Brasileira dos Bancos, Febraban, ter assinado em 27 de janeiro de 2005, um protocolo de intenções com o Instituto Nacional de Tecnologia da Informação-ITI e a Secretaria da Receita Federal para a adoção do e-CPF e do e-CNPJ **[24]**. De acordo com este protocolo os bancos se comprometem a promover o uso desses certificados entre contribuintes e usuários do sistema financeiro.

Para utilização do *smart card*, levei em consideração, além do preço do mesmo em relação ao *token*, o fato dos bancos e os usuários de serviços bancários já estarem habituados a trabalhar com cartões, além do que, caso algum banco queira estender a utilização de certificados para outros canais de atendimento, como os denominados terminais de auto-atendimento, a solução de *smart card* facilitaria esta migração, bastando para isso que as instituições substituam as atuais leitoras de cartões desses terminais por modelos que possibilitem a leitura de *smart cards*.

O e-CPF é um certificado emitido para pessoa física, pela Autoridade Certificadora da Secretaria da Receita Federal–SRF, por meio das Autoridades Certificadoras (ACs) por

ela habilitadas. Atualmente são três as ACs autorizadas pela SRF para emitir certificados e-CPF: **[25]**

- Autoridade Certificadora Certisign;
- Autoridade Certificadora Serpro;
- Autoridade Certificadora Serasa.

Apesar destes certificados também poderem ser armazenados em *tokens*, a Receita Federal por meio da publicação da Instrução Normativa SRF nº 462, de 19 de outubro de 2004, aprovou os leiautes de referência dos cartões inteligentes (*smart cards*) para armazenamento de certificados digitais e-CPF e e-CNPJ. O e-CNPJ é um certificado emitido para pessoa jurídica e não é objeto deste trabalho.

Figura 22 – Leiaute dos cartões e-CPF e e-CNPJ

A título de ilustração, foi pesquisado no mercado o preço e as opções praticadas pelas Autoridades Certificadoras que comercializam Certificados Digitais do tipo e-CPF no padrão A3.

	Certificado e-CPF A3 (validade de 3 anos) + Smart Card + Leitora	Certificado e-CPF A3 (valiade de 3 anos) em Token criptográfico USB	Certificado e-CPF A3 (validade de 3 anos) + Smart Card	Certificado e-CPF A3 (validade de 3 anos)
SERASA	R$350,00*	-	-	-
SERPRO	-	-	-	R$125,00
CERTISIGN	R$350,00	R$410,00	R$200,00	R$150,00

Fonte: www.certisign.com.br, www.serpro.gov.br e www.serasa.com.br, consulta realizada em 05.03.2006

***Certificado com validade de 2 anos.

Tabela 2 – Preços de certifcados digitais ICP Brasil do tipo A3 e-CPF

Mesmo com o protocolo firmado entre a Febraban, a Receita Federal e o ITI, até o momento nenhum dos 5 principais bancos do país (Bradesco, Itaú, Banco do Brasil, Caixa Econômica e Unibanco) ainda disponibilizaram a seus clientes soluções de autenticação em seus serviços de *internet banking* para uso exclusivo com certificados digitais no modelo proposto. O elevado custo desses certificados e a pequena quantidade de usuários da tecnologia ainda são fatores que contribuem para a baixa adesão da solução pelos bancos. Nos últimos 2 anos foram emitidos apenas cerca de 200 mil certificados digitais no padrão ICP Brasil, entretanto, especialistas prevêem a partir deste ano a consolidação da Certificação Digital no Brasil, principalmente por parte das instituições financeiras que passaram a utilizar o certificado para validar transações financeiras. **[26]**

8.3 O desenvolvimento da aplicação

8.3.1 Computador e Sistema Operacional utilizados

O computar utilizado para a realização do trabalho e implementação da simulação tem a seguinte configuração:

- Processador Intel Pentium III - 751 MHz.
- 512 MB de RAM.
- HD 60 GB.
- Sistema Operacional Windows XP – Service Pack 2.
- Porta USB (para utilização da leitora de *smart card*).
- Drive de CD (para a instalação dos softwares necessários).

A escolha de um sistema operacional da Microsoft deveu-se aos seguintes motivos:

- A leitora de *smart card* utilizada na simulação é da marca Gemplus, modelo GemPC Twin. Essa leitora possui driver de instalação que funciona melhor em várias distribuições do Windows, como 98, 98SE, Me, 2000 e XP. Já para o Linux, o driver está limitado às distribuições Redhat WS3.0, WS4.0, Suse Professional 9.2, DEBIAN "Sarge" **[27]**;

- Compatível com diversas ferramentas de desenvolvimento para linguagem Java;
- Os sistemas operacionais da Microsoft são ainda os mais utilizados no país e, portanto, de maior aceitação pelo usuário.

8.3.2 Características do certificado utilizado

Para realização do trabalho foi necessário adquirir um certificado digital do tipo e-CPF, armazenado em smart card, e uma leitora de *smart card*. O certificado foi emitido pela Autoridade Certificadora Certisign SRF e tem validade de três anos, contado a partir de 02 de março de 2006.

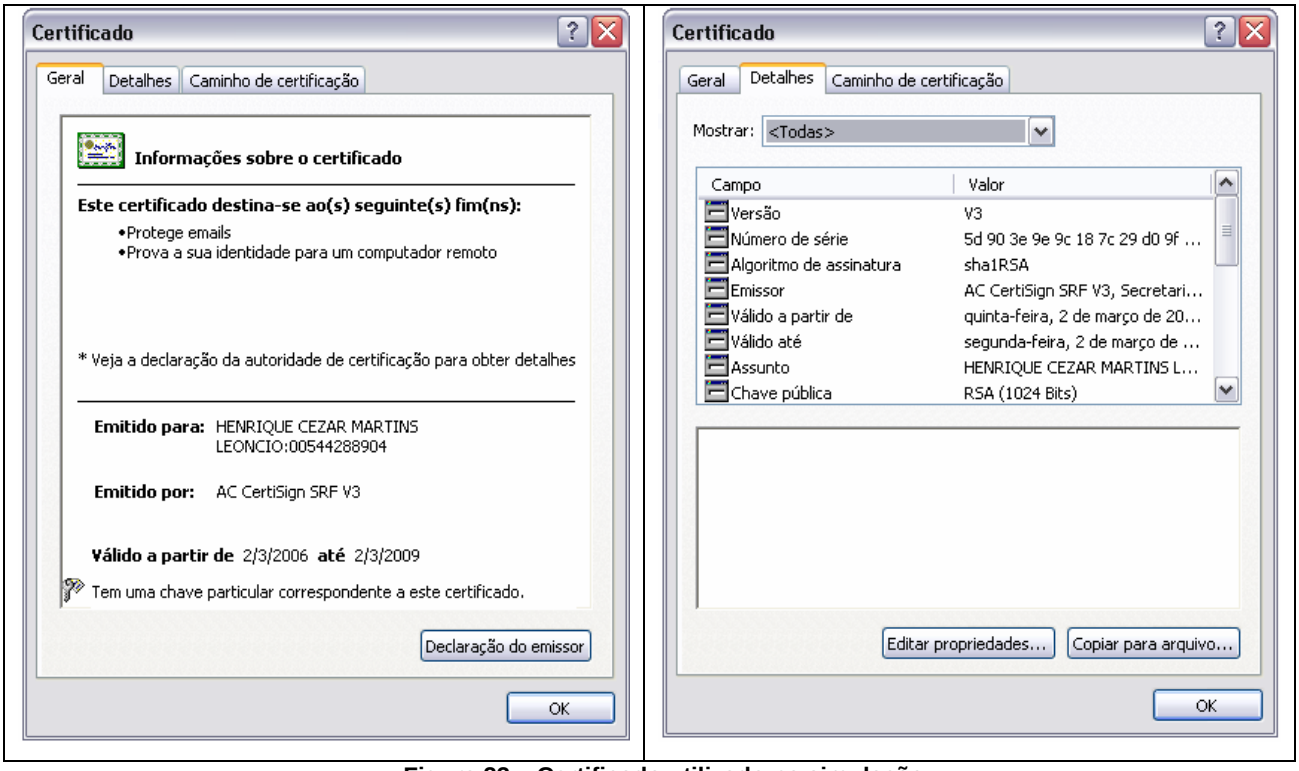


Figura 23 – Certificado utilizado na simulação

8.3.3 Driver da Leitora e CSP do cartão

Tanto o *smart card* quanto a leitora de *smart card* utilizada no trabalho são da empresa Gemplus. Para permitir o gerenciamento do cartão e reconhecimento da leitora pelo sistema operacional, foi necessário instalar o programa GemSafe Toolbox fornecido pela mesma empresa.

Por meio dessa ferramenta é possível realizar as seguintes funções:

- Leitura e gravação de dados no cartão;
- Importação e exportação de certificados;
- Gerenciamento das senhas do cartão:
  - PIN User: utilizada para proteger a Chave Privada do Certificado;
  - PIN Admin: utilizada para desbloquear o cartão após cinco tentativas erradas do PIN User.
- Gerenciamento do espaço de memória do cartão.

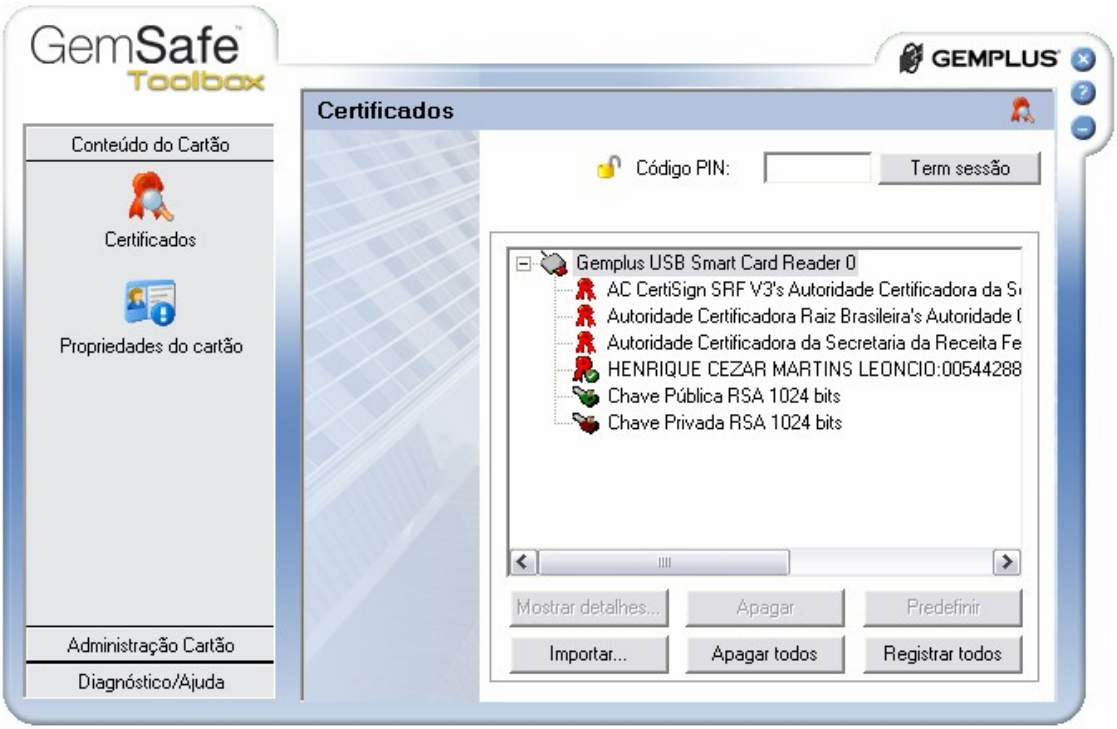


Figura 24 – Interface da ferramenta utilizada para o gerenciamento do cartão

8.3.4 Instalação da Cadeia de Raízes

A instalação da cadeia de raízes é necessária para identificar a hierarquia de confiança ou caminho da certificação utilizado no reconhecimento de um certificado. No caso de certificados ICP Brasil, devem ser instalados, obrigatoriamente, os certificados da AC Raiz Brasileira (ITI) e da Autoridade Certificadora (AC) responsável pela emissão. Caso a AC responsável pela emissão esteja hierarquicamente vinculada a uma outra AC, ela é chamada de AC de segundo ou terceiro nível, dependendo do caso. Nestas situações também é preciso armazenar o certificado das demais Autoridades Certificadoras, ou seja, deve-se percorrer todo o caminho a partir da AC Raiz até a AC responsável pela emissão do certificado. No caso do certificado utilizado neste trabalho, foram instaladas as raízes da AC Raiz, da AC SRF e da AC CertisignSRF.

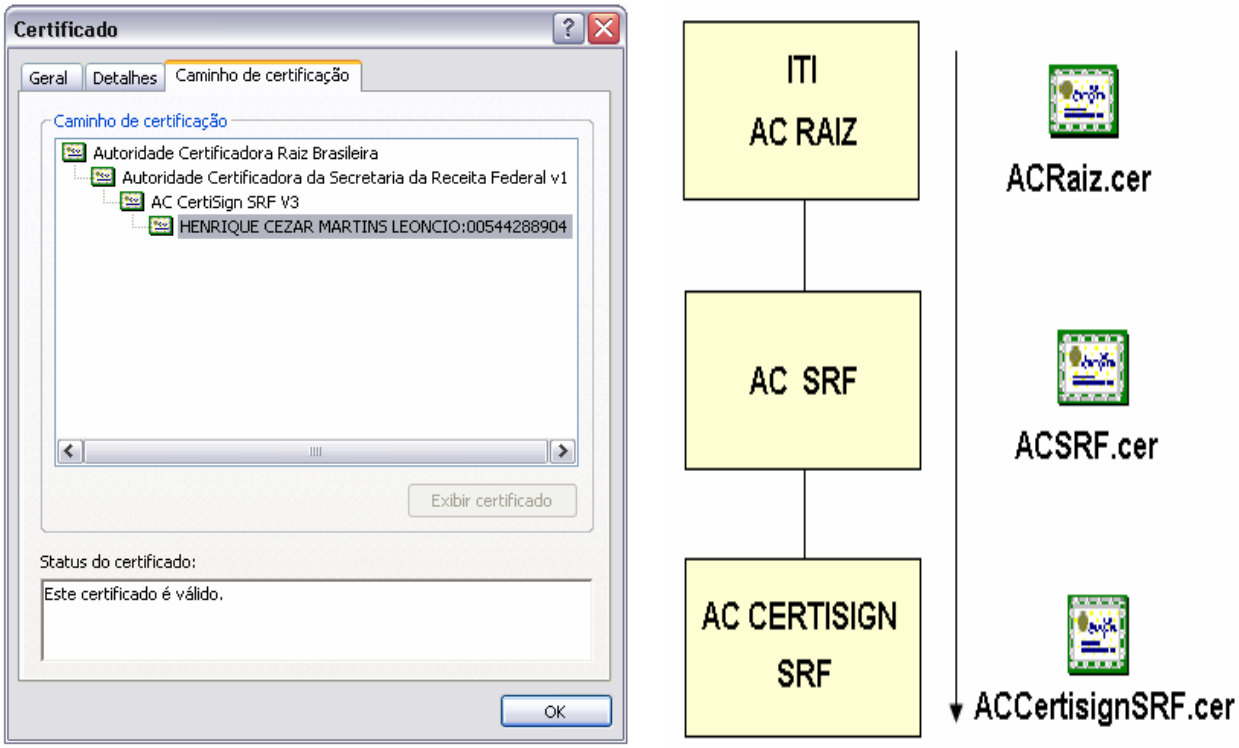


Figura 25 – Cadeia de Raízes

A instalação das raízes foi feita a partir do *site* da Autoridade Certificadora Certisign, observando as instruções do Guia de Instalação das Raízes ICP Brasil, disponível no mesmo *site*. Os arquivos de certificados digitais têm a extensão *.cer* ou *.p7b* e são armazenados em

um repositório do computador. No Windows, é possível acessar esse repositório por meio do Painel de Controle, Opções de Internet, guia Conteúdo na opção Certificados.

8.3.5 Pré-requisitos para a solução proposta

Os pré-requisitos para o funcionamento da solução são:

- Que o cliente da instituição financeira já possua um certificado digital ICP Brasil do tipo A3, armazenado em *smart card* e devidamente instalado no seu computador pessoal.
- Que o certificado seja previamente cadastrado na instituição financeira e vinculado a determinada agência e conta-corrente.

A número da agência e conta-corrente utilizados na simulação são:

- Agência: 1234
- Conta-corrente: 123456

É necessário vincular o certificado a determinada agência e conta-corrente pelos seguintes motivos:

- O cliente pode ter mais de uma conta-corrente no mesmo banco e, neste caso pode movimentar apenas uma pela internet.
- O cliente pode ter mais de um certificado digital, armazenado ou não no mesmo *smart card*, e emitido por diferentes Autoridades Certificadoras. Diante disso precisa informar ao banco qual deles irá utilizar para movimentar sua conta pela internet.

Antes de aceitar o certificado do cliente, a instituição financeira precisa validá-lo, verificando se este é um certificado ICP Brasil do tipo A3, se foi devidamente assinado pela Autoridade Certificadora que o emitiu e se a cadeia de raízes é válida. Esta verificação não é apresentada neste trabalho, mas será proposta como trabalho futuro.

De posse do certificado é possível vincular as informações como número de série do certificado, período de validade do certificado, chave pública do certificado e CPF do titular do

certificado à agência e conta-corrente do cliente. Isto é imprescindível para realizar as validações necessárias no momento em que o cliente for acessar sua conta.

Para armazenar essas informações, foi utilizado o banco de dados MySQL, que é bastante robusto, amplamente utilizado e gratuito.

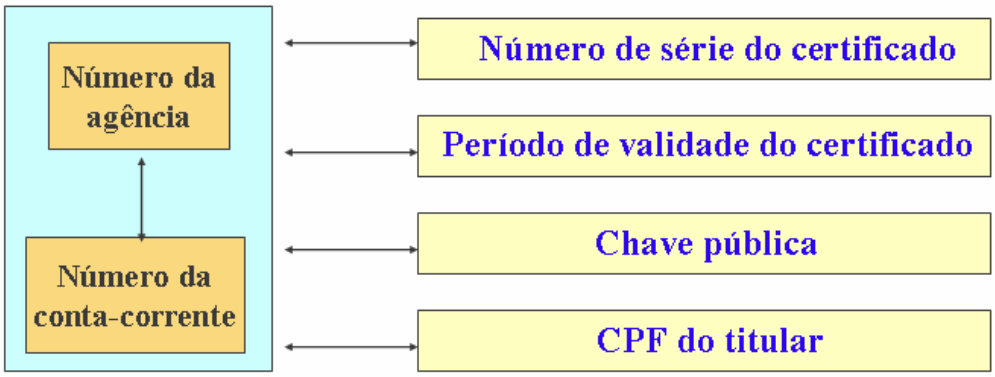


Figura 26 – Principais informações do certificado armazenadas no banco de dados

Além dessas informações, também foi armazenado no Banco de Dados a lista de certificados revogados ou LCR, que é o mecanismo utilizado por uma AC para revogar um certificado antes que este tenha seu período de validade expirado. Consiste na inserção do número serial deste certificado em um documento eletrônico chamado *Lista de Certificados Revogados (LCR)*. Portanto, uma LCR contém uma relação de todos os certificados revogados que uma AC emitiu e que ainda não tenham expirado **[28]**.

As LCR são públicas, e sua finalidade é permitir que usuários verifiquem se um certificado específico está ou não revogado. As Autoridades Certificadoras são responsáveis por disponibilizar as informações de revogação dos certificados em um local denominado repositório de certificados revogados, cabendo aos usuários que farão uso desses certificados verificar essas informações para validar um certificado recebido. Devido a importância da sua função, é essencial que as LCR sejam regularmente atualizadas, a fim de evitar que certificados revogados sejam considerados válidos por motivo de desatualização da LCR. No caso de certificados ICP Brasil do tipo A3, a LCR é atualizada pela AC de hora em hora.

8.3.6 A aplicação Java utilizada para a autenticação do usuário

A estrutura central da solução proposta esta no desenvolvimento de uma *applet* Java que é carregada junto com uma página HTML para validar o usuário que esta acessando a conta com certificado digital. Uma *applet* é um programa Java que pode ser inserido numa página web e é executado ao carregar essa página num *browser*.

É a *applet* que irá receber os dados de entrada, como número da agência, número da conta e a senha do *smart card*. Também é responsável por fazer a conexão com o banco de dados Mysql e com a API Java.

Como a instituição financeira não armazena a senha do *smart card*, utilizada para acessar a chave privada do certificado e para permitir a assinatura de documentos, a comprovação da autenticidade do usuário é verificada com sua chave pública correspondente, após o mesmo assinar com a respectiva chave privada determinada transação, neste caso uma texto qualquer, carregado junto com a *applet*.

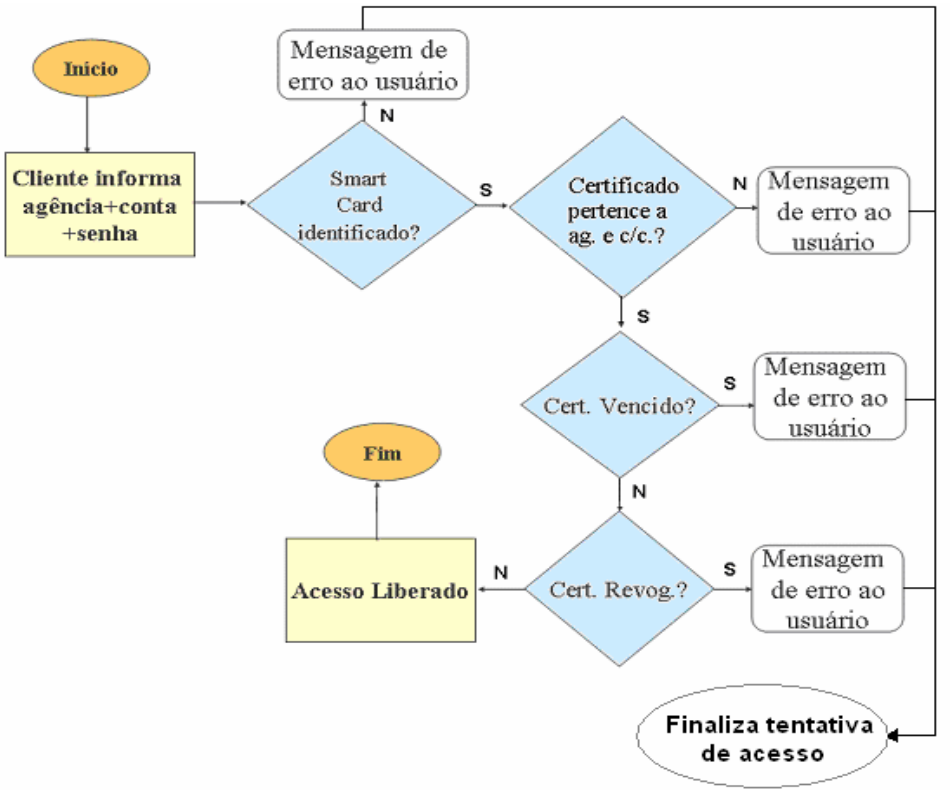


Figura 27 – Fluxograma lógico das validações realizadas

As validações apresentadas na simulação foram realizadas observando-se os seguintes critérios:

- **Identificação do *smart card e* senha:** neste caso, o teste foi realizado após ser informado para a aplicação o número da agência, da conta-corrente e da senha do *smart card*, porém sem o cartão estar inserido na leitora. A aplicação retorna para o usuário a mensagem “Verifique se o cartão encontra-se na leitora ou se a senha confere”. A mesma mensagem é apresentada se o cartão estiver na leitora e for informado somente o número da agência e da conta-corrente, sem a senha do *smart card*.

- **Certificado vinculado à agência e conta informada**: este teste teve como objetivo mostrar que o sistema é capaz de identificar uma tentativa de acesso indevida, realizada após ser informado como entrada para a aplicação a senha do *smart card* e um número de agência ou conta-corrente diferente daqueles vinculados ao certificado utilizado. A aplicação retorna para o usuário a mensagem “Certificado não pertence à agência/conta informada”.

- **Validade do certificado:** para verificar se um certificado está ou não vencido, a instituição financeira deve comparar o período de validade deste com a data atualizada do momento em que o usuário tenta acessar sua conta com o certificado. Esta verificação deve ser efetuada para cada tentativa de acesso. Como o certificado utilizado na simulação tem validade até o dia 02 de março de 2009, o teste para mostrar uma tentativa de acesso com um certificado vencido foi realizado após se alterar a data do equipamento para uma data posterior ao dia 02 de março de 2009. A aplicação retorna para o usuário a mensagem “Certificado vencido”.

- **Certificado revogado:** uma das obrigações da instituição financeira que queira aceitar a utilização de certificados digitais por parte de seus clientes é manter atualizada a lista de certificados revogados disponibilizada periodicamente pelas Autoridades Certificadoras. Para mostrar uma tentativa de acesso a conta-corrente com um certificado cadastrado, porém revogado, foi necessário incluir este certificado em uma tabela do banco de dados utilizada para representar a lista de certificados revogados armazenada pela instituição financeira. Neste caso a aplicação retorna para o usuário a mensagem “Certificado revogado”.

Para a manipulação do algoritmo de criptografia do certificado digital, que é um RSA de 1048 bits, foram utilizadas classes da *Bouncy Castle*, que é uma biblioteca de criptografia para aplicações Java. Um dos fatores levados em conta para utilização destas classes foi o fato de terem sido amplamente testadas pelo mercado. Também permitem trabalhar de forma rápida com criptografia assimétrica, além de garantir a compatibilidade com o padrão de certificados X.509.

A segurança do algoritmo RSA é baseada na dificuldade computacional de se fatorar um número inteiro em números primos, portanto, está diretamente relacionada com o tamanho dos números primos utilizados. Hoje em dia os números primos mais utilizados têm 512 bits de comprimento e combinados formam chaves de 1024 ou de 2048 bits. **[22] [29]**

Desde que se tornou público, o algoritmo RSA vem sendo amplamente testado e, até hoje, tem se mostrado bastante útil e seguro em várias aplicações e protocolos que exigem segurança, entre eles: **[30]**

- Certificados de Segurança;
- Assinaturas Digitais;
- S/Mime e PGP;
- protocolo SSL, TLS e IPSec.

Os certificados digitais do tipo A3 utilizam o algoritmo RSA de 1048 bits no processo de assinatura digital.

Para o desenvolvimento da aplicação foi utilizado o Ambiente de Desenvolvimento Integrado, IDE Eclipse, por ser esta uma ferramenta neutra em linguagem de desenvolvimento, por apresentar inúmeros plug-ins voltados para a linguagem Java, pela variedade de recursos disponíveis e principalmente por ser de uso gratuito.

A opção pela linguagem Java foi devido ao fato desta ser uma linguagem completa e adequada para o desenvolvimento de aplicações baseadas na internet. Outras características importantes de Java, que também ajudaram na sua escolha são: **[31]**

- Portabilidade: independência de plataforma de hardware e software;
- Fornece suporte a orientação a objetos permitindo a modularização das aplicações e a reutilização do código já implementado;
- Permite a criação de programas robustos e seguros:
- Traz classes para o suporte a vários níveis de conectividade como acesso a URLs (padrão Internet), uso de conexões em *sockets*, criação de protocolos, criação de clientes e servidores.

Devido a essas características e principalmente pela independência de plataforma e ampla quantidade de bibliotecas existentes, escolheu-se a linguagem Java. Vale ressaltar, entretanto, que outras linguagens de programação, como o C ou C++, poderiam ser utilizadas. Esta decisão, porém, teria como conseqüência uma aplicação limitada a determinada plataforma, além de um impacto maior no desenvolvimento do projeto.

8.3.7 As páginas HTML

Com o objetivo de simular o acesso ao site de uma instituição financeira e para carregar a applet utilizada na autenticação do usuário, foram criadas três páginas em HTML. Uma vez que a solução pode ser adotada por qualquer banco e para não particularizarmos a proposta para um banco específico, foi criado um nome fictício de banco denominado “Banco Local”.

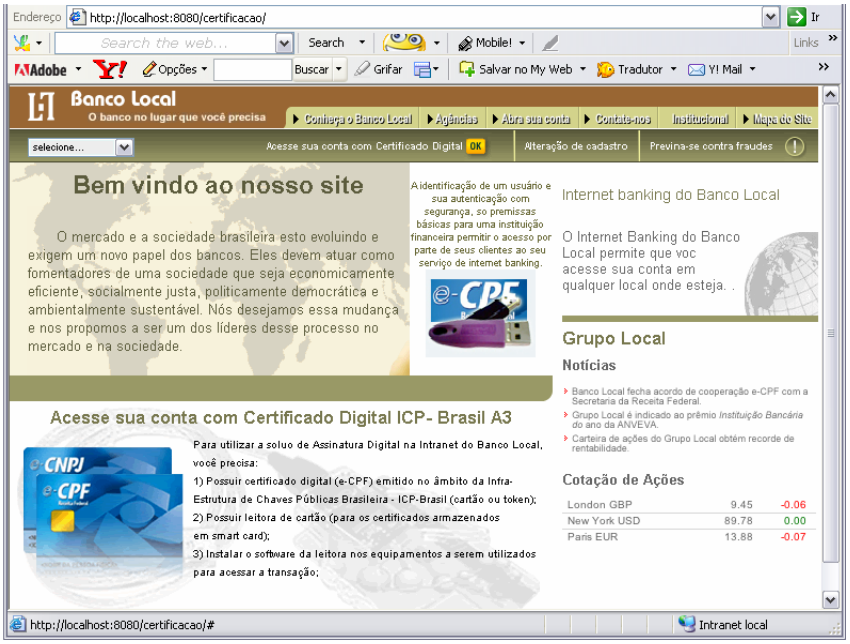


Figura 28 – Página HTML utilizada para representar o site de um banco qualquer

Essa página contém um *link* para acesso a conta-corrente do usuário com certificado digital do tipo A3. Após clicar neste link o usuário é direcionado para uma outra página que carrega a *Applet* Java, conforme mostrado na figura abaixo.

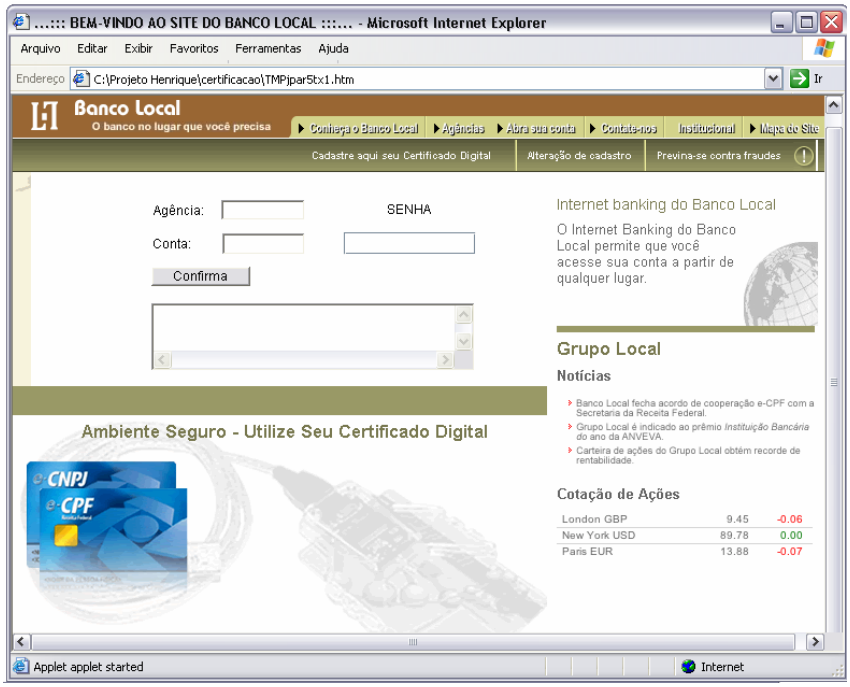


Figura 29 – Página HTML utilizada para carregar a applet de autenticação

Caso o usuário consiga assinar a transação, o acesso a sua conta-corrente será liberado. Foi utilizado um nome fictício para o cliente denominado “João da Silva”.

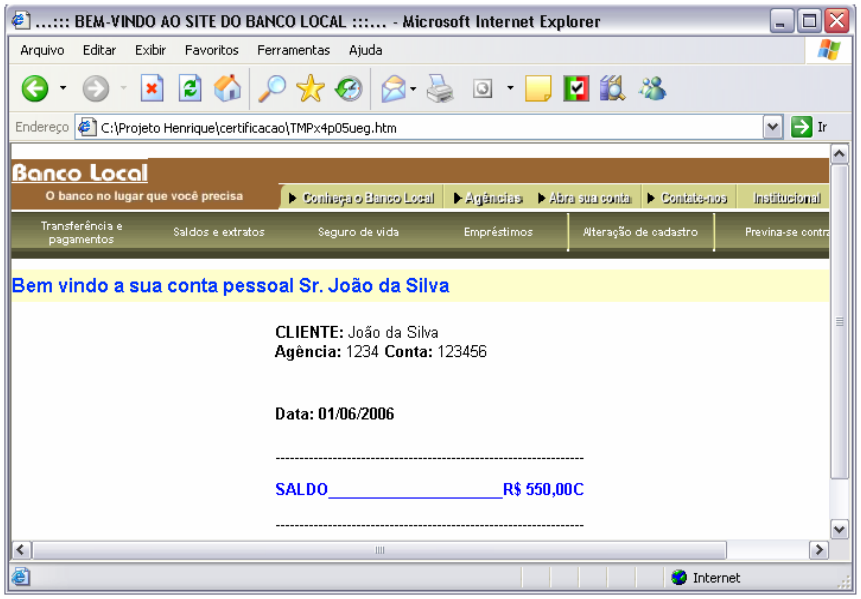


Figura 30 – Página HTML apresentada após a liberação do acesso

8.3.8 O Servidor Web utilizado

Para armazenar as páginas desenvolvidas foi utilizado o servidor web Apache-Tomcat. A principal característica deste servidor é que o mesmo está centrado na linguagem de programação Java, mais especificamente na tecnologia de Java Server Pages (JSP). Portanto, para carregarmos as páginas HTML no servidor foi necessário mudar a extensão das mesmas para arquivos com extensão jsp. Uma página escrita em JSP é uma página escrita em HTML e que contém pequenos fragmentos de código Java. O Tomcat é capaz de criar código fonte Java a partir de um documento HTML.

Em termos práticos, o Tomcat pode ser usado isoladamente, assumindo o papel de um servidor web, ou em conjunto com outro servidor, como por exemplo o Apache. Neste caso, o Apache atende a requisições de páginas estáticas enquanto que o Tomcat atende a requisições de páginas dinâmicas.

Também foi levado em consideração para a escolha do Apache-Tomcat o fato deste ser gratuito, estar disponível em várias plataformas e em constante evolução.

8.3.9 Dificuldades encontradas e suas soluções

Foram várias as dificuldades encontradas durante o desenvolvimento deste trabalho, entre as quais é relevante destacar:

- Pouca literatura técnica sobre certificados digitais ICP Brasil: esta deficiência foi resolvida por meio de consulta a profissionais da área e da participação em cursos e seminários sobre o assunto.
- Pouco conhecimentos sobre a linguagem Java: para minimizar este problema foi necessário contar com a ajuda de colegas do curso, além da participação em fóruns de discussão e cursos específicos sobre Java.
- Custo dos materiais: o preço do certificado utilizado, acompanhado da leitora e do *smart card* foi de R$350,00 (trezentos e cinqüenta reais).

8.4 Vantagens e desvantagens da solução proposta

A solução apresentada traz vantagens tanto para o cliente, usuário dos serviços de *internet banking*, quanto para a instituição financeira que resolver adotá-la. O principal ganho para o cliente é que este estará mais seguro aos ataques de programas maliciosos do tipo cavalo-de-tróia, pois mesmo que um programa desta natureza consiga capturar sua senha, não será possível realizar nenhuma transação, pois ainda haverá a necessidade de estar com o cartão do cliente. Para o banco, os principais benefícios estão relacionados ao aumento de credibilidade junto aos clientes e à redução das perdas financeiras decorrentes de fraudes nesse canal.

Para os bancos, porém, a solução apresenta algumas desvantagens, como a periodicidade da publicação da lista de certificados revogados, pois o tempo de publicação da LCR de hora em hora é extremamente crítico para uma instituição financeira, uma vez que neste intervalo um certificado pode ter sido revogado e ser utilizado indevidamente por alguém não autorizado. Outra desvantagem é a pequena quantidade de usuários de certificados ICP-Brasil do tipo A3, que ainda são muito caros, o que implica em uma

pequena parcela de clientes com condições de adquiri-lo. Portanto, o investimento no desenvolvimento de uma solução desta natureza pode não justificar.

9. Conclusão

As soluções de segurança que vêm sendo adotadas pelos bancos para acesso aos seus serviços de internet banking têm se mostrado ineficientes para combater as fraudes nesse canal. Com a proposta apresentada neste trabalho foi possível demonstrar que a utilização de Certificados Digitais ICP Brasil do tipo A3 por clientes de instituições financeiras, além de ser viável de ser implementada, pode agregar segurança no processo de autenticação.

A segurança dessa tecnologia associada ao rigoroso processo de emissão de um certificado na ICP Brasil traz vantagens tanto para o usuário que passará a utilizar com mais frequência a internet para a realização de transações financeiras como para o banco, que terá mais credibilidade junto ao mercado e aos seus clientes, além de reduzir suas perdas financeiras decorrentes de fraudes no canal internet.

Por meio da simulação apresentada foi possível demonstrar as principais validações que devem ser realizadas antes de se liberar o acesso ao serviço de internet banking para um cliente titular de um Certificado Digital ICP Brasil.

Como o número de usuários de certificados digitais no Brasil ainda é pequeno, principalmente em função do custo dos certificados, os bancos têm como alternativa fornecer esses certificados a todos os seus clientes usuários do internet banking. Para isso podem optar por tornar-se ou uma Autoridade de Registro ou uma Autoridade Certificadora na ICP Brasil.

Pelas várias iniciativas já adotadas no País para a utilização de Certificados Digitais ICP Brasil e, principalmente pela formalização do protocolo de intenções entre a Febraban, o ITI e a Receita para adoção dos certificados e-CPF e e-CNPJ, pode-se concluir que a proposta apresentada pode vir a tornar-se em breve uma realidade entre os bancos.

10. Trabalhos Futuros

O assunto abordado neste trabalho permite a realização de outras pesquisas relacionadas ao tema que podem agregar melhorias na solução proposta ou serem apresentadas como um novo trabalho. São elas:

- Propor e apresentar um solução que mostre o cadastramento e a validação dos certificados do cliente na instituição financeira.
- Propor e apresentar uma solução que mostre a assinatura de outras transações relacionadas aos serviços de *internet banking* oferecidos pelos bancos, como transferências entre contas e pagamentos de títulos. Estas transações seriam apresentadas ao cliente de tal forma que ele possa assiná-las com seu Certificado Digital do tipo A3. O cliente também poderia recuperar todas as transações assinadas com seu certificado digital.
- Apresentar estudo sobre os terminais de auto-atendimento utilizados pelos bancos e como estes poderiam ser adaptados para aceitar a utilização de certificados ICP Brasil do tipo A3, armazenados em *smart card*.
- Propor e apresentar uma solução web que possibilite assinar arquivos com certificado digital ICP Brasil do tipo A3 e enviá-los a um terceiro previamente cadastrado de forma segura.

11. Referências bibliográficas

[1] SOUZA, TULIO CICERO S. **Aplicações Embarcadas para Gerenciamento de Chaves Criptográficas.** Universidade Federal de Santa Catarina, Junho, 2005. Monografia de Graduação.

[2] HIGA, F. A.; MURR, J. A. N. **Certificação Digital.** Universidade Federal do Rio Grande do Sul - Porto Alegre, dezembro, 2002. Monografia para obtenção do grau de Especialista em Informática.

[3] SILVA, BRUNO DE MELO. **Uma abordagem de infra-estrutura de chaves públicas para ambientes corporativos**. Centro Universitário de Brasília, junho de 2004. Monografia de graduação para obtenção do grau de bacharel em Engenharia da Computação.

[4] NETO, AMÉRICO CORDEIRO V. e CALDEIRA, RENATA M. **Autenticação de usuários em serviços web de instituições financeiras**, Monografia de Graduação, UNB, fevereiro de 2004

[5] VALOR. Jornal Valor on-line. Disponível em: <http://www.valor.com.br/>. Acesso em: Abril, 2006.

[6] COMPAGNO, R. **GERAÇÃO AUTOMÁTICA DE POLÍTICAS PARA DETECÇÃO DE INTRUSÕES BASEADA EM EVIDÊNCIAS DE ATAQUE**. Universidade de Campinas - Unicamp, dezembro, 2005. Tese de Mestrado.

[7] CID, D. B. **Métodos de Autenticação.** Disponível em: <http://www.ossec.net/docs/sec/auth.html>. Acesso em: Março, 2006.

[8] Cartilha de Segurança para Internet – Parte I: Conceitos de segurança. Disponível em: <http://cartilha.cert.br/conceitos/sec2.html#subsec2.1>. Acesso em: Março, 2006.

[9] DE HOLANDA FERRERIA, A. B. **Dicionário Aurélio Eletrônico Século XXI**. Versão 3.0. ed. Novembro, 1999.

[10] KAZIENKO, J. F. **Assinatura Digital de Documentos Eletrônicos Através da Impressão Digital.** Universidade Federal de Santa Catarina, fevereiro, 2003. Tese de Mestrado.

[11] CTIS. Loja de Informática CTIS. Disponível em: <http://www.lojactis.com.br/busca_nova.asp?busca=impress%E3o+digital&loja=>. Acesso em: Março, 2006.

[12] CERT.BR. **Cartilha de Segurança para Internet**. Disponível em: <http://cartilha.cert.br/>. Acesso em: Abril, 2006.

[13] SYMANTEC. Disponível em: <http://www.symantec.com>. Acesso em: Abril, 2006

[14] LINHARES, D. **Aplicação de Técnicas de Forense Computacional e Respostas a Incidentes na Internet**. Brasília, 2004. Especialização em Segurança em Redes de Computadores.

[15] INFOGUERRA. Site sobre segurança. Disponível em: <http://www.infoguerra.com.br/infonews/viewnews.cgi?newsid1029191691,76456>. Acesso em: Abril, 2006.

[16] BRASIL. **Medida Provisória N. 2.200-2, de 24.08.2001**. Disponível em: <http://www.iti.gov.br/medidaprovisoria.htm>. Acesso em: Janeiro, 2006.

[17] ITI. **Instituto Nacional de Tecnologia da Informação**. Disponível em: <http://www.iti.br/twiki/bin/view/Main/AutCerti>. Acesso em: Fevereiro, 2006.

[18] BRASIL. Resolução n. 7, de 12 de dezembro de 2001. Aprova os requisitos mínimos para políticas de certificado na ICP-Brasil. Comitê Gestor da ICP-Brasil.

[19] SILVA, Lino Sarlo da. **Public Key Infrastructure – PKI – Conheça a Infra-estrutura de Chaves Públicas e a Certificação Digita**. São Paulo: Editora Novatec, 2004.

[20] BURNETT, Steve. **Criptografia e Segurança – O Guia Oficial RSA**. Rio de Janeiro: Editora Campus, 2002.

[21] ITI. Resoluções. Disponível em: <http://www.iti.gov.br/resolucoes.htm>. Acesso em: Abril, 2006.

[22] MORENO, Edward David. **Criptografia em Software e Hardware**. São Paulo: Editora Novatec, 2005.

[23] VIANNA, PAULO. **Certificação Digital e mobilidade**. Disponível em: <http://www.certisign.com.br/certinews/destaques/materia_14.jsp>. Acesso em: Fevereiro, 2006.

[24] ITI. Instituto Nacional de Tecnologia da Informação. Disponível em: <http://www.iti.br/>. Acesso em: Março, 2006.

[25] SRF. Secretaria da Receita Federal. Disponível em: <www.receita.fazenda.gov.br>. Acesso em: Março, 2006.

[26] REVIEW. Revista Security Review. **Autenticidade em Ascensão.** Edição n. 6 ano II, p.52-57, Janeiro/feveiro, 2006.

[27] GEMPLUS. Empresa Gemplus – Fabricante de smart cards e de leitoras de smart cards. Disponível em <http://www.gemplus.com/products/gempctwin/>. Acesso em: Fevereiro, 2006.

[28] VIEGA, J.; MESSIER, M.; CHANDRA, P. *Network Security with OpenSSL*. [S.l.]: O'Reilly, 2002.

[29] COUTINHO, S, C. **Números inteiros e criptografia RSA**. Rio de Janeiro:

IMPA/SBM, 2000.

[30] BARBOSA, LUIZ. et al. **RSA Criptografia Assimétrica e Assinatura Digital**.. Universidade Estadual de Campinas, Julho, 2003. Especialização em Redes de Computadores.

[31] DEITEL,H.M., DEITEL,P.J., **Java - Como Programar.** 3º Ed. - Editora Bookman, 2001.

Anexos

Anexo A - Código Fonte da Applet Java

```
/*
 * Autor: Henrique Cezar Martins Leoncio
 */

package validacoes;

import java.applet.Applet;
import java.awt.Button;
import java.awt.Label;
import java.awt.TextArea;
import java.awt.TextField;
import java.net.MalformedURLException;
import java.net.URL;
import javax.swing.JOptionPane;
import javax.swing.JPasswordField;
import javax.swing.SwingUtilities;

public class AppletAcesso extends Applet {

	private Label label = null;
	private Label label1 = null;
	private Label label2 = null;
	private TextField agencia = null;
	private TextField conta = null;
	private Button button = null;
	private JPasswordField senha = null;

	private TextArea saida = null;

	/**
	 * Inicializa agência
	 */
	private TextField getAgencia() {
		if (agencia == null) {
			agencia = new TextField();
			agencia.setBounds(new java.awt.Rectangle(81, 15, 78, 19));
		}
		return agencia;
	}

	/**
	 * Inicializa conta
	 */
	private TextField getConta() {
		if (conta == null) {
			conta = new TextField();
			conta.setBounds(new java.awt.Rectangle(82, 46, 77, 20));
```

```
		}
		return conta;
	}
	private Button getButton() {
		if (button == null) {
			button = new Button();
			button.setBounds(new java.awt.Rectangle(16, 77, 92, 18));
			button.setLabel("Confirma");
			button.addActionListener(new java.awt.event.ActionListener() {
			public void actionPerformed(java.awt.event.ActionEvent e) {

			SwingUtilities.invokeLater(new Runnable() {
			public void run() {
			SmartCard sc = new SmartCard();
			String result = sc.initAutorizacao(getSenha().getText().toCharArray(), new
Integer( getAgencia().getText()),
			new Integer( getConta().getText()));
			getSaida().setText(result);
			System.out.println(result);
			if (!"Sucesso".equals(result)) {
			JOptionPane.showMessageDialog(null, "Problemas na execucao de sua
transacao\n\n" + result);
			getAgencia().setText("");
			getConta().setText("");
			getSenha().setText("");
			} else {
			redireciona();
				}
			}
				});
			}
			}
			);
		}
		return button;
	}

	/**
	 * Inicializa senha
	 */
	private JPasswordField getSenha() {
		if (senha == null) {
			senha = new JPasswordField();
			senha.setBounds(new java.awt.Rectangle(195, 45, 123, 21));
		}
		return senha;
	}

	public AppletAcesso() {
	  super();
	}
```

```
	public void init() {
		label2 = new Label();
		label2.setBounds(new java.awt.Rectangle(195, 15, 122, 18));
		label2.setAlignment(java.awt.Label.CENTER);
		label2.setText("SENHA");
		label1 = new Label();
		label1.setBounds(new java.awt.Rectangle(15, 45, 63, 21));
		label1.setText("Conta:");
		label = new Label();
		label.setBounds(new java.awt.Rectangle(16, 15, 63, 19));
		label.setText("Agência:");
		this.setLayout(null);
		this.setSize(347, 191);
		this.setBackground(new java.awt.Color(255,255,230));
		this.add(label, null);
		this.add(label1, null);
		this.add(label2, null);
		this.add(getAgencia(), null);
		this.add(getConta(), null);
		this.add(getButton(), null);
		this.add(getSenha(), null);
		this.add(getSaida(), null);
	}

	private TextArea getSaida() {
		if (saida == null) {
			saida = new TextArea();
			saida.setBounds(new java.awt.Rectangle(16,111,321,45));
		}
		return saida;
	}

	/**
	 * Método que redireciona para página  pessoal do cliente
	 */
	private void redireciona() {
		try {
			getAppletContext()
					.showDocument(
							new URL(

	"http://localhost:8080/certificacao/paginaCliente.jsp"));
		} catch (MalformedURLException e) {
			e.printStackTrace();
		}

	}
}
```

Anexo B - Código Fonte dos métodos de autenticação

```
/**
 * Autor: Henrique Cezar Martins Leoncio
 *
 */


package validacoes;

import java.applet.Applet;
import java.io.InputStream;
import java.security.KeyStore;
import java.security.PrivateKey;
import java.security.Provider;
import java.security.Security;
import java.security.Signature;
import java.security.cert.X509Certificate;
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.Statement;
import java.util.Enumeration;

import org.bouncycastle.util.encoders.Base64;

public class SmartCard {

	public SmartCard() {
		super();

		InputStream in = this.getClass().getResourceAsStream("/pkcs11.config");
		p = new sun.security.pkcs11.SunPKCS11(in);
	}

	/**
	 * Inicializacao dos providers. São necessarios para o reconhecimento do
	 * smart card.
	 */
	private sun.security.pkcs11.SunPKCS11 p;
	private KeyStore.PasswordProtection pp;

	/** String que será assinada com a chave privada do titular do certificado
	 * cadastrado. Se a chave pública armazenada conseguir decifrar a mensagem
	 * assinada, a autenticidade estará comprovada.
	 */
	String protocolo = "STRING QUE SERÁ ASSINADA";

	KeyStore.Builder builder = null;
```

```
	/**
	 * Método que inicializa a verificação completa do smart card do cliente.
	 * (assina a string, verifica a agencia e a conta, se o certificado
	 * corresponde ao armazenado, se esta vigente e se não esta revogado).

	 * Parametros: senha do smart card, número da agência e número da conta
	 *
	 */
	public String initAutorizacao(char[] pin, int agencia, int conta){
		System.out.println("Inicializando providers...");
		Provider bounc = new org.bouncycastle.jce.provider.BouncyCastleProvider();
		Security.addProvider(p);
		Security.addProvider(bounc);

		/*Cria instancia para utilizar o cartao. Abstrai o store onde esta o
		certificado.*/
		this.pp = new KeyStore.PasswordProtection(pin);
		KeyStore.Builder.newInstance("pkcs11",p ,pp);
		builder = KeyStore.Builder.newInstance("pkcs11",p ,pp);
		try{
			System.out.println("Inicializando store...");
			//Repositorio de chaves
			KeyStore ks = builder.getKeyStore();
			ks.load(null, pin);

			//Captura o certificado no smart card
			String certCliente = getCertificado();

			//Assinatura da string
			byte[] assinaturaCliente = geraAssinatura(ks, pin);

			//Efetua as validacoes para a conta e as validacoes do certificado.
			if(validadeCertificado()){
				System.out.println("Certificado com data válida.");
				if (verificaAutenticacao(agencia, conta, assinaturaCliente)){
					System.out.println("Certificado autorizado a utilizar a conta");
					if(!verificaLCR(certCliente)){
						System.out.println("Certificado não está revogado");
						System.out.println("Certificado autorizado a operar
transacoes");
					}else{
						System.out.println("Certificado revogado");
						return "Certificado revogado";
					}
				}else{
					System.out.println("Certificado não pertence a agência/conta
informada");
					return "Certificado não pertence a agência/conta informada";
				}
			}else{
```

```
                        System.out.println("Certificado Vencido.");
                        return "Certificado Vencido";
                    }

                }catch(Exception ex){
                    ex.printStackTrace();
                    return "Verifique se o cartão encontra-se na leitora ou se a senha confere";
                }
                return "ACESSO LIBERADO";
        }

        /**
         * Metodo que busca o certificado que está no smart card.
         */

        private String getCertificado(){
                /* BASE 64: codificação que faz a representação de um array de bytes em formato
string.
                */
                String certBase64;
                try{
                    KeyStore store = builder.getKeyStore();
                    Enumeration en = store.aliases();
                    String cert = (String)en.nextElement();
                    X509Certificate ctfd = (X509Certificate)store.getCertificate(cert);
                    certBase64 = new String(Base64.encode(ctfd.getEncoded()));
                    //Função que retorna o Certificado codificado em Base64
                    return certBase64;
                }catch(Exception e){
                    //Erro ao acessar o cartao
                    e.printStackTrace();
                }
                return null;
        }
        **
         * Método que verifica se o certificado está vencido ou não
         */
        private boolean validadeCertificado(){
                try{
                    KeyStore store = builder.getKeyStore();
                    Enumeration en = store.aliases();
                    String cert = (String)en.nextElement();
                    X509Certificate ctfd = (X509Certificate)store.getCertificate(cert);
                    try{
                        //Valida o certificado
                        ctfd.checkValidity();
                        return true;
                    }catch(Exception ex){
                        return false;
                        //Certificado vencido
                        //ex.printStackTrace();
```

```
                }
        }catch(Exception e){
                //Erro ao acessar o certificado no cartão
                e.printStackTrace();
        }
        return false;
}

/**
 * Método que gera a assinatura utilizando a chave privada do smart.
 * Não existe acesso a chave privada, ocorre apenas a assinatura de uma string
 * Esse dado assinado será usado para verificar se o certificado que está na
 * base corresponde ao do cliente.
 *
 * @param ks
 * @param pin
 * @return byte[] assinatura
 */
private byte[] geraAssinatura(KeyStore ks, char[] pin){
        try{
                PrivateKey priv = (PrivateKey)ks.getKey(ks.aliases().nextElement(), pin);
                Signature sign = Signature.getInstance("SHA1withRSA", p);
                sign.initSign(priv);
                sign.update(protocolo.getBytes());
                byte[] dadoAssinado = sign.sign();
                return dadoAssinado;
        }catch(Exception e){
                //Erro na assinatura
                e.printStackTrace();
        }
        return null;
}

/**
 * Método que verifica se a agência e a conta conferem com o certificado do cliente.
 * Primeiro, o sistema verifica se existe aquela agência e conta associada.
 * Em seguida utiliza a assinatura do cliente para verificar se o certificado
 * é o correto.
 *
 * @param agencia
 * @param conta
 * @param dadoAssinado
 * @return
 */
private boolean verificaAutenticacao(int agencia, int conta, byte[] dadoAssinado){
        boolean resultado = false;
        Connection connection;
        //Query do SQL - Verifica apenas se a agencia e conta existem.
        String query =
                "SELECT * FROM clientes WHERE agencia='"
                + agencia + "' AND conta='"
```

```
                + conta + """;
        try{
                Class.forName("com.mysql.jdbc.Driver");
                connection =
                        DriverManager.getConnection("jdbc:mysql://localhost:3306/conta",
"root", "");
                Statement statement = connection.createStatement();
                ResultSet result =
                        statement.executeQuery(query);
                if(result.next()){

                        //Captura o  certificado associado a agência e conta.
                        String certB64 = result.getString("certificado");

                        //Formata o certificado no padrão X.509
                        byte[] certByte = Base64.decode(certB64);
                        javax.security.cert.X509Certificate cert =
                                javax.security.cert.X509Certificate.getInstance(certByte);

                        /* Verifica a assinatura utilizando o texto que está no inicio do
                         * codigo e o certificado armazenado na base.
                         */
                        try{
                                Signature sign = Signature.getInstance("SHA1withRSA");
                                sign.initVerify(cert.getPublicKey());
                                sign.update(protocolo.getBytes());
                                resultado = sign.verify(dadoAssinado);
                        }catch(Exception ex1){
                                System.err.println("Nao foi possivel verificar a assinatura");
                                ex1.printStackTrace();
                        }

                        return resultado;
                }else{
                        System.out.println("Agencia ou conta não incorreta.");
                }
                result.close();
                statement.close();
                connection.close();
        }catch(Exception e){
                //Erro ao acessar o banco de dados
                e.printStackTrace();
        }
        return resultado;
    }


    /**
     * Metodo que verifica se o certificado está ou nao na tabela de LCR
     * parâmetro: certificado
     */
```

```
	public boolean verificaLCR(String certificado){
		boolean resultado = false;
		Connection connection;
		String query =
			"SELECT * FROM lcr WHERE certbase64='"
			+ certificado + "'";
		try{
			Class.forName("com.mysql.jdbc.Driver");
			connection =
				DriverManager.getConnection("jdbc:mysql://localhost:3306/conta",
"root", "");

			Statement statement = connection.createStatement();
			ResultSet result =
				statement.executeQuery(query);
			if(result.next()){
				//System.out.println("Certificado revogado.");
				resultado = true;
				return resultado;
			}
			result.close();
			statement.close();
			connection.close();
		}catch(Exception e){
			//Erro ao acessar o banco SQL
			e.printStackTrace();
		}
		return resultado;
	}
}
```