PLATAFORMA DE DESENVOLVIMENTO PINHÃO PARANÁ

MANUAL DE CONFIGURAÇÃO DO NAVEGADOR MOZILLA FIREFOX

Agosto – 2006

Sumário de Informações do Documento

Tipo do Documento: Manual
Título do Documento: MANUAL DE CONFIGURAÇÃO DO NAVEGADOR MOZILLA/FIREFOX
Estado do Documento: EB (Elaboração)
Responsáveis: Emerson Sachio Saito
Palavras-Chaves: Mozilla, Firefox, leitor, Smart, Card, Certificado, Digital
Resumo: Manual de configuração do Mozilla/Firefox para uso de Certificados Digitais.
Número de páginas: 20
Software utilizados: BR-Office Writer

Versão	Data	Mudanças
1.0	28/08/2006	Criação (Revisão: Cíntia A Evangelista)
1.1	07/02/2006	Houve alteração na página da Raiz da ICP-BRASIL

SUMÁRIO

1 INTRODUÇÃO

Este manual destina-se a orientar a configuração do navegador Mozilla/Firefox, para uso de certificados digitais, armazenados em arquivos que são os de nível A1 e S1, os armazenados em hardware criptográfico que são os de nível A3,S3,A4 e S4 (token ou smart-card).

O ambiente operacional homologado é o LINUX/DEBIAN.

O documento não detalhará nenhum conceito de certificação digital ou das ferramentas relacionadas, pois estes conhecimentos são considerados pré-requisitos para este manual.

2 PRÉ-REQUISITOS BÁSICOS

- Conceitos de Certificação Digital: A plataforma de desenvolvimento PINHÃO fornece material e cursos para aquisição destes conhecimentos.
- Navegador Mozilla Firefox 1.5 ou superior.
- Instalação do pacote mozilla-opensc, que é o pacote para uso da biblioteca OPENSC, pode ser feita preferencialmente pela interface gráfica SYNAPTIC ou por comando de linha: APT-GET INSTALL.
- Certificado digital padrão ICP-BRASIL.
- Cadeias de certificados da autoridade emissora, seus respectivos emissores e principalmente a cadeia RAIZ da IPC-BRASIL.

3 CONFIGURAÇÃO DAS AUTORIDADES CERTIFICADORAS.

A primeira configuração a ser executada, é a inserção das cadeias de certificados das autoridades certificadoras, que correspondem ao certificado emitido.

Existem duas maneiras de fazer esta configuração: Automaticamente através do portal internet da autoridade certificadora ou por Configuração Manual.

3.1 Automaticamente através da página Internet da autoridade certificadora

Esta maneira é mais fácil e confiável, abaixo seguem os passos para a configuração:

Primeiramente deve-se conhecer os endereços de internet (url) da autoridade certificadora e as demais informações por ela fornecidas referentes à certificação digital.

Executar/abrir o navegador Mozilla Firefox e digitar o endereço da autoridade certificadora correspondente ao certificado adquirido, que neste exemplo é a da CEF (Caixa Econômica Federal) http://icp.caixa.gov.br.

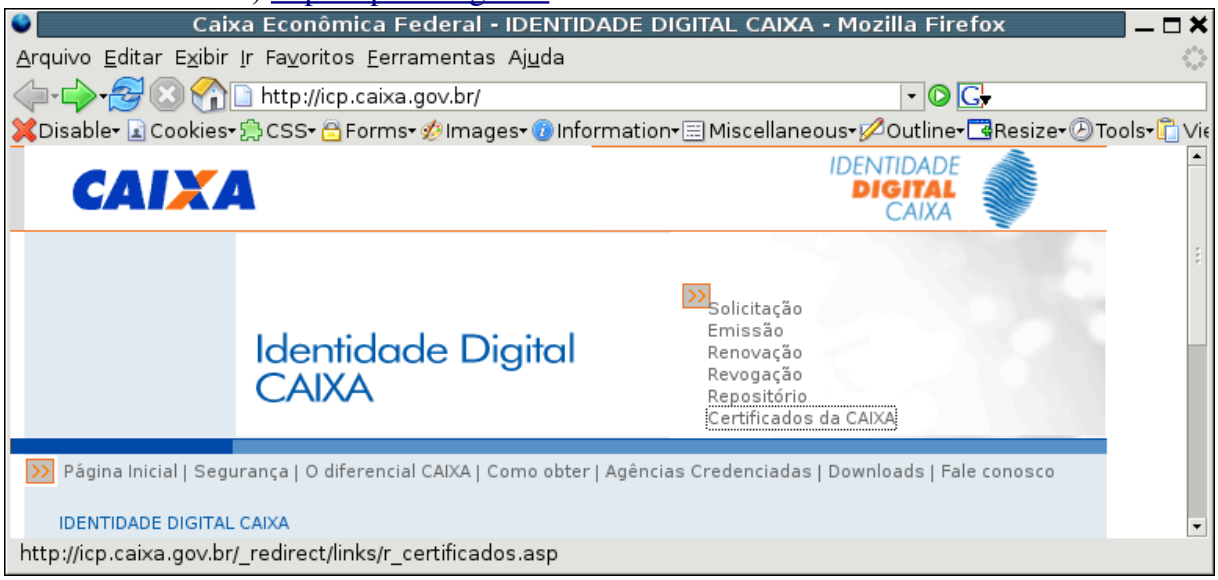

Figura 1 – Portal da Autoridade Certificadora em Agosto de 2006.

Em seguida entrar na página que armazena os certificados (esta informação é obtida com a autoridade) que neste caso é o link: Certificados da CAIXA.

Figura 2 – Certificados da Autoridade Certificadora – Em agosto de 2006.

O primeiro certificado a ser inserido é o da ICP-BRASIL, não haverá problemas mesmo que já tenha sido inserido anteriormente, basta clicar sobre o link Certificado Digital da AC Raiz Brasileira que abrirá a seguinte tela:

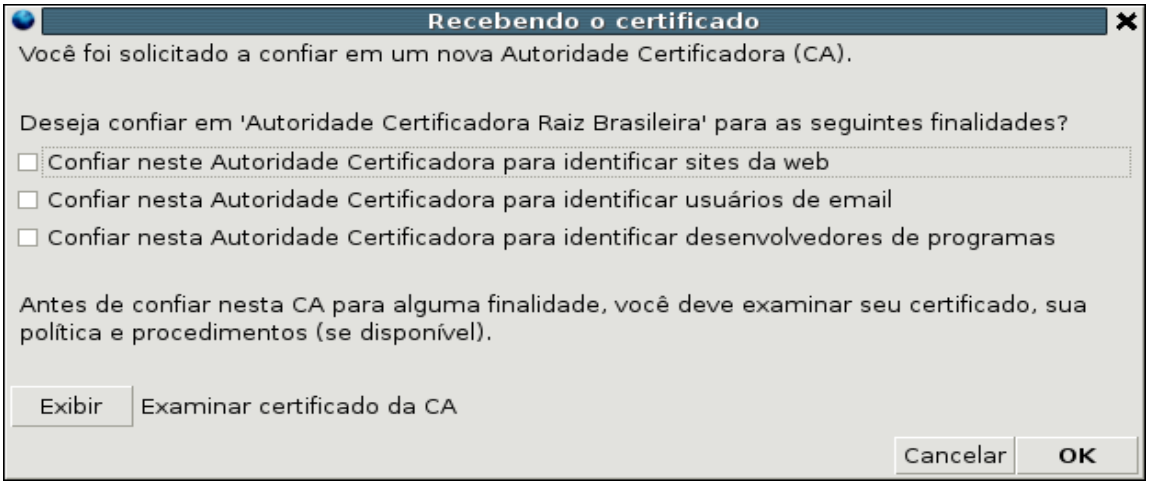

Figura 3 – Recebendo o certificado.

Marcar todas as opções de confiança e finalidades e clicar no botão OK.

Este passo será repetido, mas agora para o restante da cadeia, que são as AC's de níveis inferiores ao da Raiz e conforme a sua hierarquia.

Neste exemplo a seqüência é a seguinte:

- Certificado Digital da AC Caixa
- Certificado Digital da AC Caixa - Pessoa Física

A figura 3 será reapresentada nos dois casos e deverão ser marcadas todas as opções também.

Com isto as cadeias estarão incluídas. E caso queira confirmar selecione o menu Editar/Preferências (ou teclas alt+E+P), que irá abrir a tela de preferências.

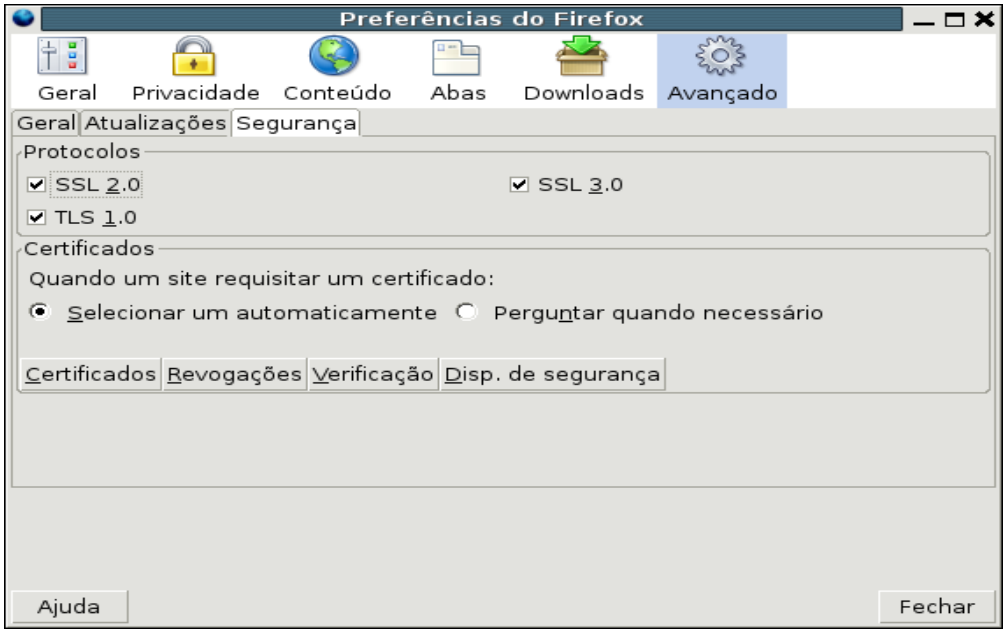

Figura 4 – Preferências do Firefox.

Na seqüência clicar no ícone **Avançado** e depois na aba **Segurança,** em seguida clicar na opção **Certificados** que irá apresentar a tela do Gerenciador de Certificados, depois clicar na aba **Autoridades**:

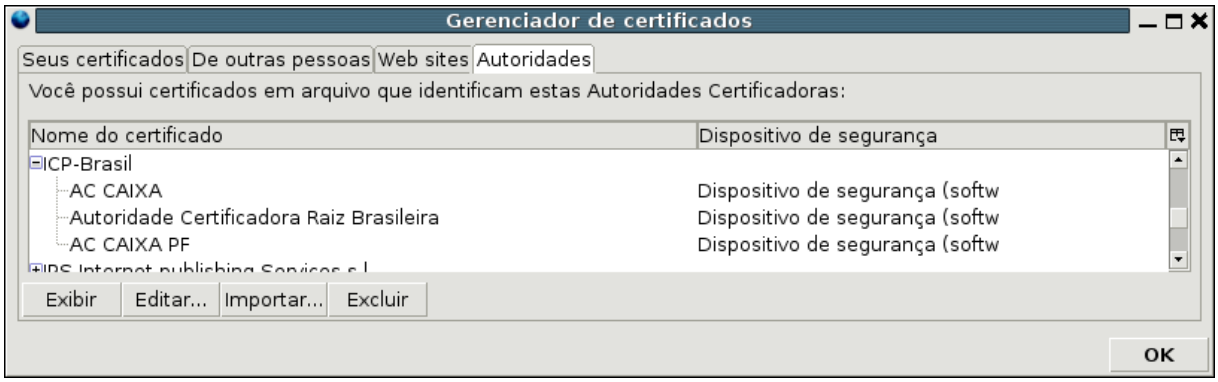

Figura 5 – Gerenciador de Certificados – Destaque para as autoridades incluídas da ICP-BRASIL

3.2 Configuração Manual

Para a configuração manual é preciso dos arquivos(.cer) dos certificados das autoridades, que deverão estar em um diretório acessível, estes arquivos devem ser fornecidos pela autoridade certificadora ou disponibilizados em um endereço/site internet.

O primeiro passo é executar/abrir o navegador Mozilla Firefox.

Selecione o menu Editar/Preferências (ou teclas alt+E+P), que abrirá a tela de preferências.

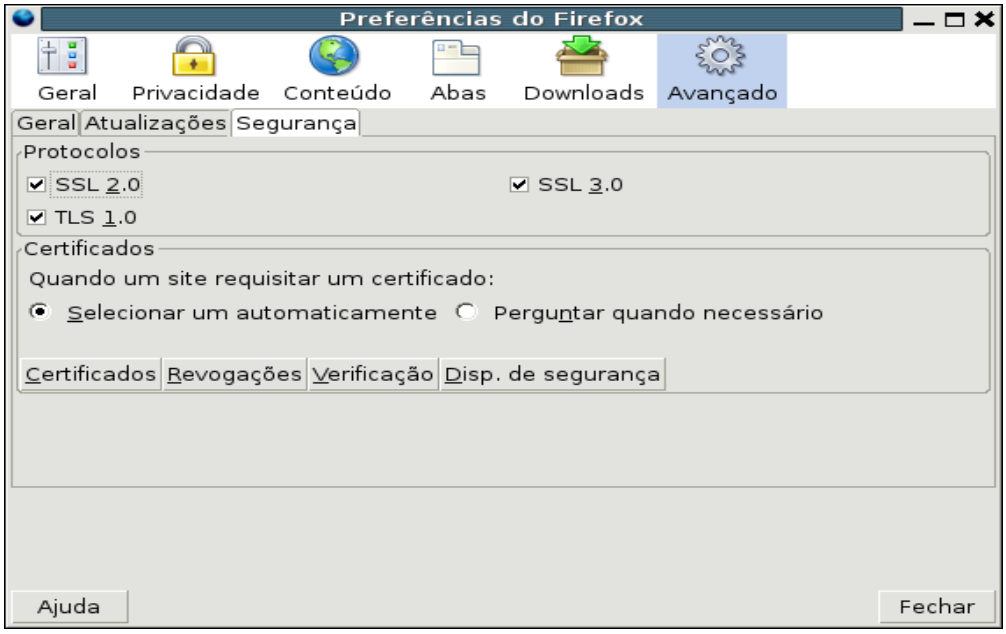

Figura 6 – Preferências do Firefox.

Na seqüência clicar no ícone **Avançado** e depois na aba **Segurança,** em seguida clicar na opção Certificados que apresentará a tela do Gerenciador de Certificados, depois clicar na aba **Autoridades** que irá apresentar a tela seguinte:

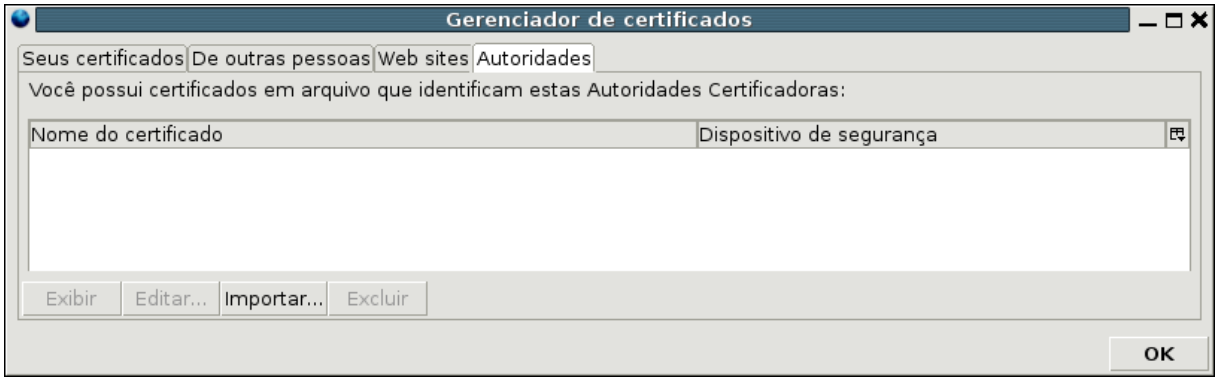

Figura 7 – Gerenciador de certificados na aba autoridades.

Clicar no botão **Importar...** e informar o diretório e o nome dos arquivos de certificados das AC's.

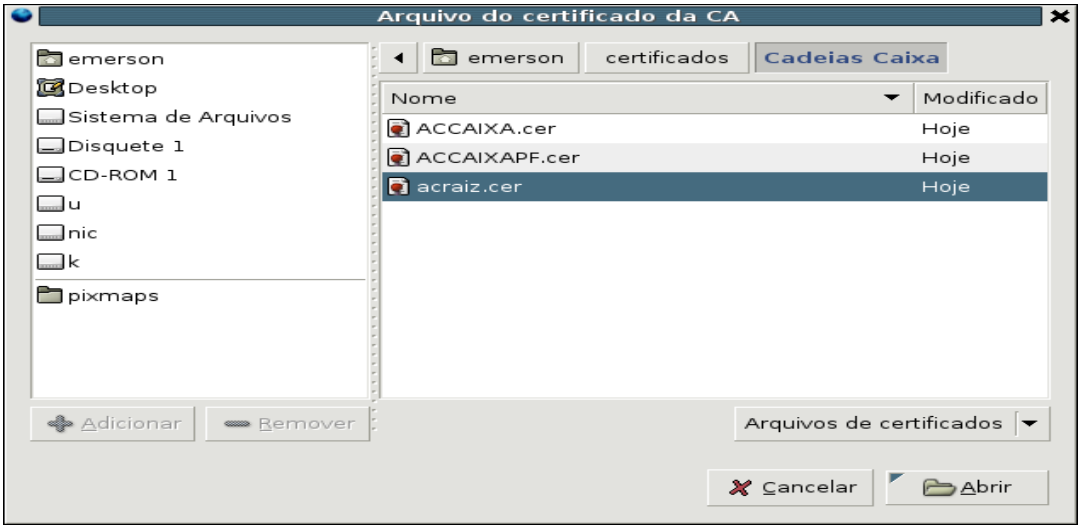

Figura 8 – Arquivos de certificados.

Será necessário repetir a tarefa para cada arquivo, conforme a hierarquia, partindo da RAIZ e marcar todas a opções de confiança e finalidades, conforme a tela abaixo:

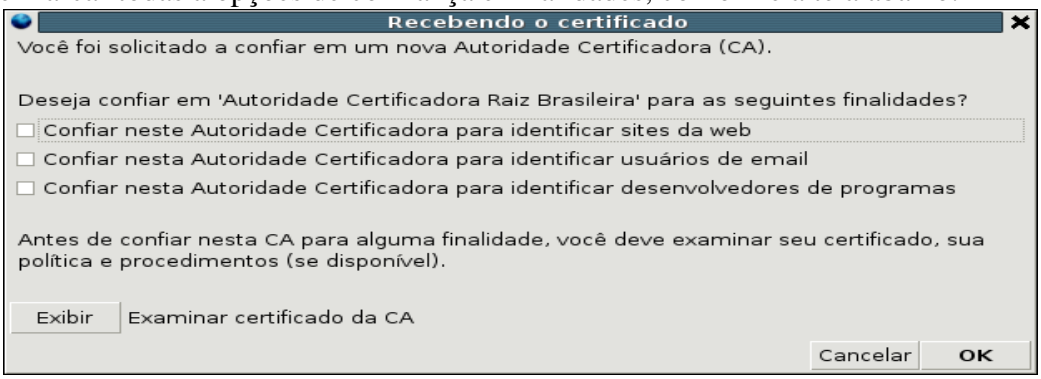

Figura 9 – Recebendo o certificado.

Executar o procedimento das figuras 7, 8 e 9 para cada arquivo armazenado, conforme a hierarquia das autoridades certificadoras.

Este procedimento só é recomendado quando não se tem conexão Internet disponível.

4 CONFIGURAÇÃO DE LISTAS DE REVOGAÇÃO.

Um procedimento importante para o uso dos certificados validados por autoridades certificadoras, é a configuração da lista de certificados revogados, que garantirá a validade do certificado para cada autoridade. Para configuração das autoridades existem duas formas conforme segue:

4.1 Automaticamente através da página internet da autoridade certificadora

Esta maneira é a mais fácil e intuitiva, basta seguir os passos seguintes:

Seguindo o padrão a primeira lista deverá ser a da RAIZ da ICP-BRASIL que se encontra no endereço: http://acraiz.icpbrasil.gov.br/

Figura 10 – Portal da Autoridade Certificadora Raiz da ICP-BRASIL em Fevereiro de 2007.

No quadro esquerdo encontra-se o link para a lista de certificados revogados(**LCR - Download**).

Basta clicar no link que irá apresentar a tela abaixo:

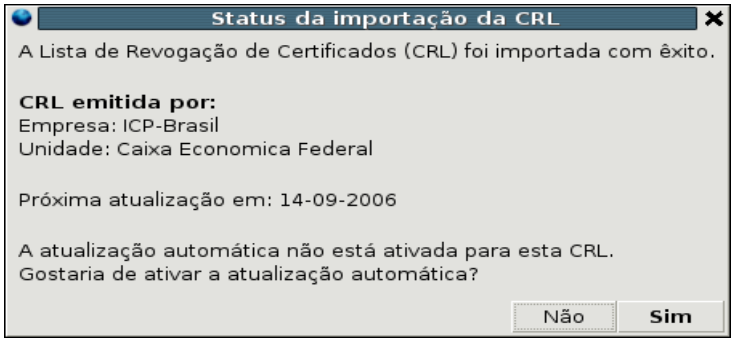

Figura 11 – Status da importação da CRL

Clicar no botão **Sim** para ativar a atualização automática da lista, que apresentará a tela seguinte:

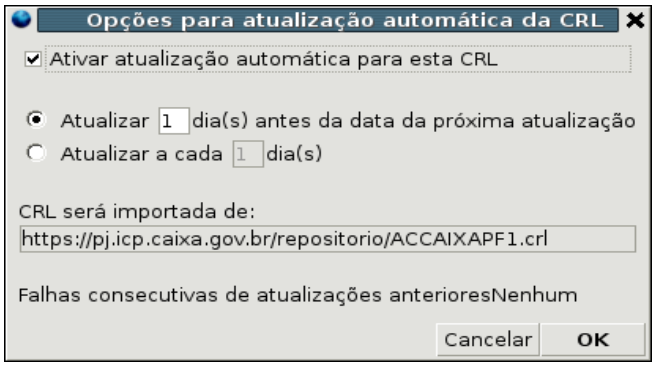

Figura 12 – Opções para atualização automática da CRL.

Assinalar a opção Ativar e clicar no botão OK. Isto fará com que a lista seja atualizada automaticamente, desde que haja conexão internet, quando o navegador é executado.

Depois é preciso conhecer o endereço internet da autoridade certificadora, que armazena as listas de certificados revogados.

Digitar o endereço da autoridade certificadora correspondente, que neste exemplo é a da CEF (Caixa Econômica Federal) https://pf.icp.caixa.gov.br/asp/repositorio.asp

Procurar os links:

☐ LCR da AC CAIXA

☐ LCR da AC CAIXA - Pessoa Física

Clicar em cada um dos links e o mesmo procedimento das figuras 11 e 12 deverá ser seguido para cada um dos links, poderão haver mais níveis de autoridades conforme o certificado.

4.2 Configuração Manual.

Na configuração manual é preciso conhecer o endereço exato para a lista de certificados revogados, por isto o item 4.1 é o mais recomendado, principalmente quando se utiliza o proxy para acesso a internet.

Seguir o item 3.2 até a figura 6., depois clicar na aba **Segurança** e em seguida clicar na opção Revogações que apresentará a tela abaixo:

Figura 13 – Gerenciador de CRL (lista de certificados revogados)

Clicar então no botão **Importar...** que exibirá a tela seguinte:

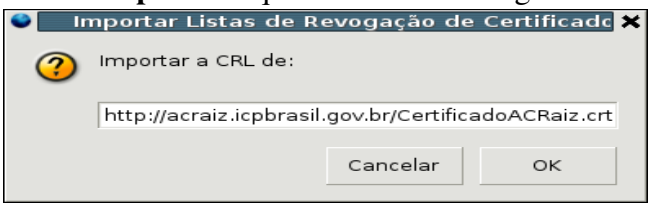

Figura 14 – Importar Listas de Revogação de Certificado

Informar o endereço completo da lista, sendo que a primeira deve ser obrigatoriamente a RAIZ da ICP-BRASIL (http://acraiz.icpbrasil.gov.br/LCRacraiz.crl).

Executar o mesmo passo para todas as autoridades conforme a hierarquia do certificado.

5 PROCEDIMENTOS PARA CERTIFICADO EM ARQUIVOS.

As aplicações WEB que utilizam certificados digitais pessoais, podem exigir um certo nível de segurança que em alguns casos pode ser suprido por um certificado de nível A1 ou S1 e nestes casos explicaremos como fazer a sua configuração no Mozilla Firefox.

5.1 Pré-requisitos.

Completar o item 3.1 ou 3.2.

Adquirir o certificado ou exportá-lo no formato PKCS12.

5.2 Configuração do certificado em arquivo.

Executar/abrir o navegador Mozilla Firefox.

Selecionar o menu Editar/Preferências (ou teclas alt+E+P), que abrirá a tela de preferências.

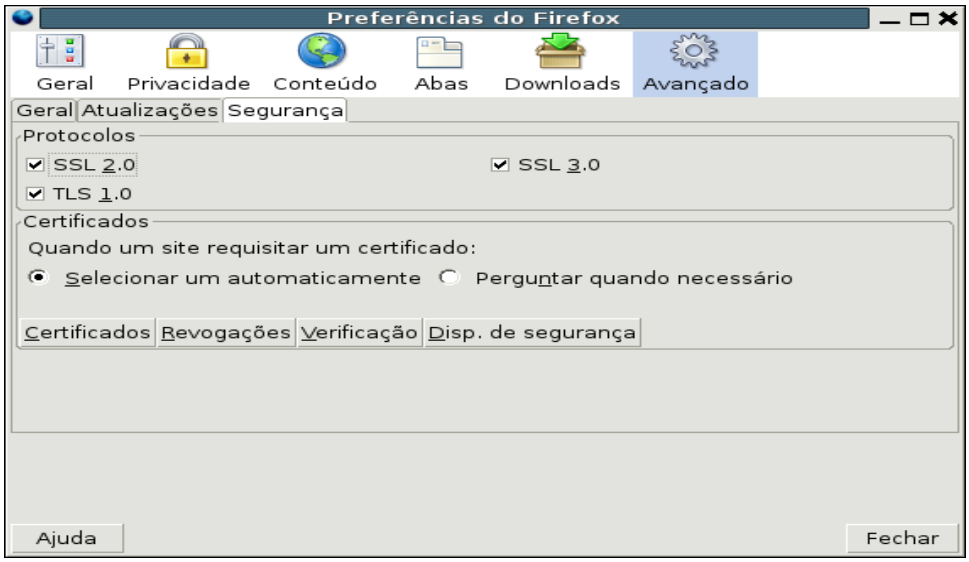

Figura 15 – Preferências do Firefox.

Na seqüência deve-se clicar no ícone **Avançado** e depois na aba **Segurança,** em seguida clicar na opção **Certificados,** que apresentará a tela do Gerenciador de Certificados, depois clicar na aba **Seus Certificados** e a tela seguinte aparecerá:

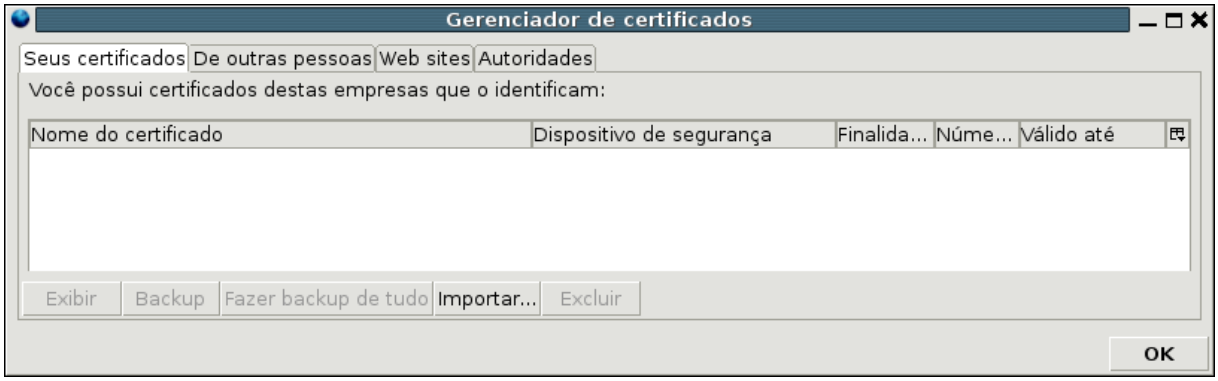

Figura 16 – Gerenciador de certificados – Destaque para Seus certificados.

Na seqüência clicar no botão **Importar...** e deve-se informar o diretório e o nome do arquivo de certificado no formato PKCS12 (.pfx ou .p12)

Será solicitada a senha para o certificado e a tela de confirmação aparecerá.

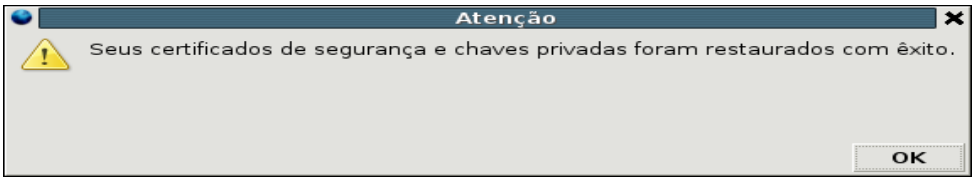

Figura 17 – Confirmação de importação.

Logo após o certificado deverá ser listado na tela da figura 11.

A partir deste momento o navegador estará preparado para acessar aplicações WEB, que utilizem certificados digitais de nível A1.

6 PROCEDIMENTOS PARA CERTIFICADOS EM HARDWARE

Os certificados digitais armazenados em hardware (níveis A2,A3, A4, S2,S3 e S4), garantem um maior nível de segurança pois utilizam dispositivos de hardware e são exigidos em muitas aplicações WEB. Neste item será orientada a Configuração deste tipo de certificado no Mozilla Firefox.

6.1 Pré-requisitos

- Instalação e configuração da leitora de SmartCard ou Token: ver arquivo **GIC_ManualInstalacaoLeitorSmartCard**
- Configuração das Autoridades Certificadoras conforme o item 3.1 ou 3.2 deste manual.
- Pacotes DEBIAN necessários:

mozilla-opensc	versão 0.11.1-1	Pacote de suporte do Mozilla (e Firebird) para o opensc

Instalar via apt-get ou Synaptic.

6.2 Configuração e Ativação.

Fechar todas as janelas ou navegadores Mozilla Firefox Abertos.

Com todos os pré-requisitos validados, certificar-se de que a Leitora de SmartCard ou Token esteja conectado ao computador, e no caso do SmartCard que o mesmo esteja inserido na Leitora.

Execute/Abra novamente o Mozilla Firefox.

Para ativar a instalação selecionar o menu Editar/Preferências (ou teclas alt+E+P), que abrirá a tela de preferências, neste momento o navegador irá procurar e configurar automaticamente o certificado, o que pode demorar alguns segundos conforme o equipamento e a instalação, em determinadas versões ou instalações o processo não é feito

automaticamente e neste caso será necessário configurar conforme será explicado na seqüência.

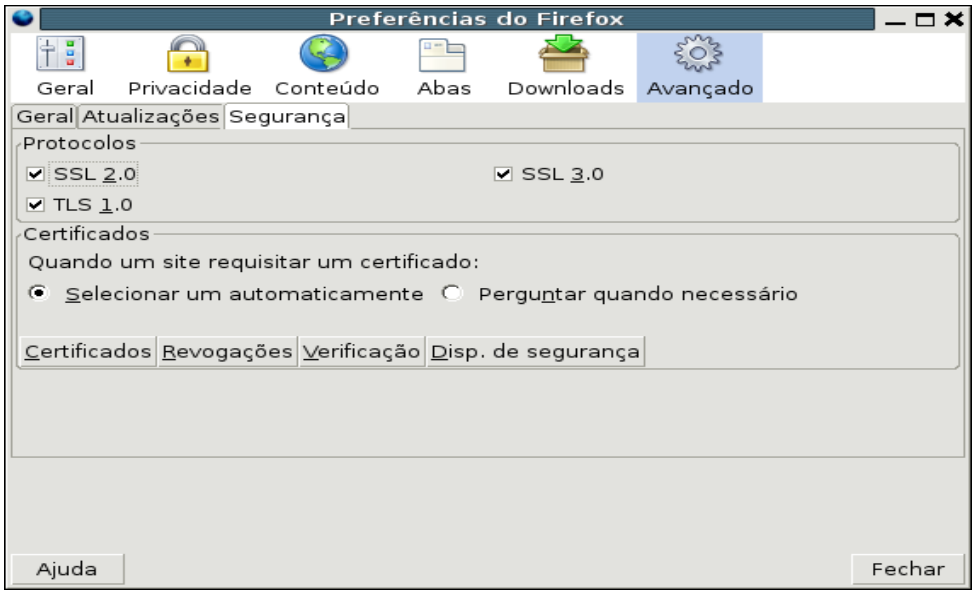

Figura 18 – Preferências do Firefox.

Para verificar a instalação e ativação do certificado clicar no ícone **Avançado** e depois na aba **Segurança,** em seguida clicar na opção **Disp. de Segurança,** que irá apresentar a tela do Gerenciador de Dispositivos de Segurança. Nesta tela deverá aparecer o certificado pessoal assim como o dispositivo de leitura:

Figura 19 - Gerenciador de Dispositivos de Segurança – destaque no certificado.

Se o certificado for listado como na figura 14, o Mozilla Firefox está habilitado para trabalhar com o certificado e acessar as aplicações que necessitem de certificado digital.

Caso o certificado não conste na lista, é porque não foi reconhecido, pois o dispositivo de leitura não foi carregado de forma automática, e neste caso será necessário o carregamento manual.

Primeiramente deve-se certificar de que o cartão esteja na leitora ou o token conectado.

Para carregamento manual, ainda na tela da figura 14, clicar no botão **carregar** que abrirá a tela abaixo:

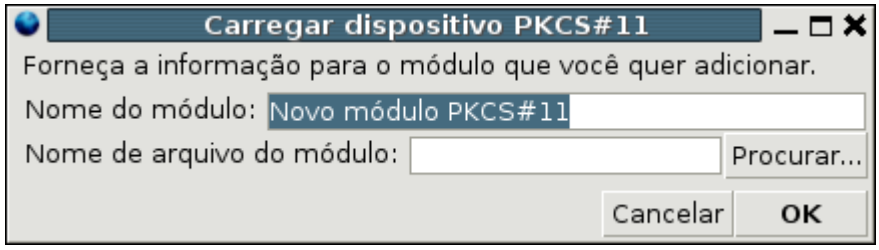

Figura 20 – Carregar dispositivo PKCS#11

Nesta tela informar o **Nome do módulo**, poderá ser qualquer nome que se consiga identificar facilmente, como por exemplo: “Minha leitora”, e em seguida informar o **Nome do arquivo do módulo,** que deverá ser: ***/usr/lib/opensc/opensc-pkcs11.so*** ou então, clicar no botão Procurar... para informar o diretório (conforme a figura 16). É a forma mais prática e também para casos onde o arquivo ***opensc-pkcs11.so*** não esteja no diretório /usr/lib/opensc.

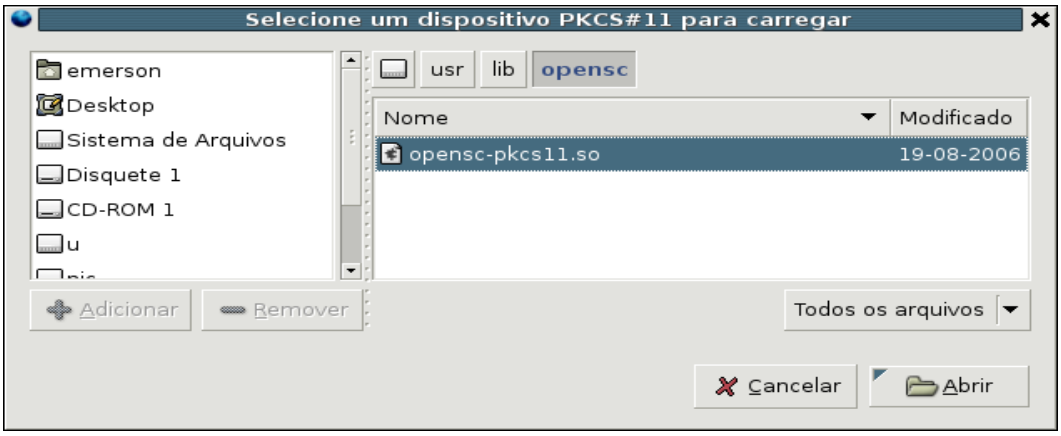

Figura 21 – Seleção do dispositivo de segurança.

Neste momento o certificado será lido e carregado, o que pode levar um certo tempo dependendo do equipamento. Após isto o certificado deverá ser listado como na figura 14, e a partir deste momento o Mozilla Firefox estará habilitado para uso do certificado digital.

Atualmente o Mozilla Firefox não pode ser utilizado em paralelo com Thunderbird para uso do SmartCard, pois o primeiro programa que fizer a leitura do certificado, irá bloquear a leitura para o outro, mas não impedirá o seu funcionamento. Portanto havendo interesse em se utilizar o certificado em ambos, a execução deverá ser em separado. Em caso de assinar e criptografar e-mails Thunderbird e utilizar o Firefox para acessar páginas que não necessitem de certificado digital, não haverá problemas.

6.3 Alteração da senha pessoal (PIN) do certificado.

Através da interface do navegador, é possível efetuar a mudança da senha pessoal do smartcard/token. Com medida de segurança e recomendado que a mesma seja alterada periodicamente.

Para isto, estando configurado conforme o item anterior, abra o navegador e execute os procedimentos das figuras 18 e 19. A tela apresentada deverá ser a seguinte:

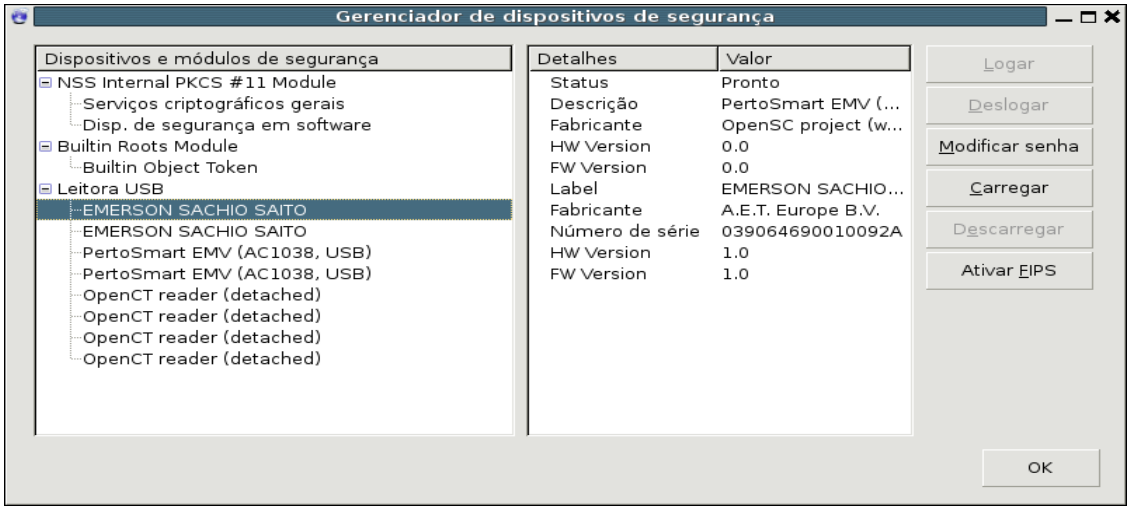

Figura 22. Gerenciador de Dispositivos de segurança.

Note que o botão **Modificar senha** deverá estar habilitado.

Clique neste botão para fazer a mudança de senha, a seguinte tela será apresentada:

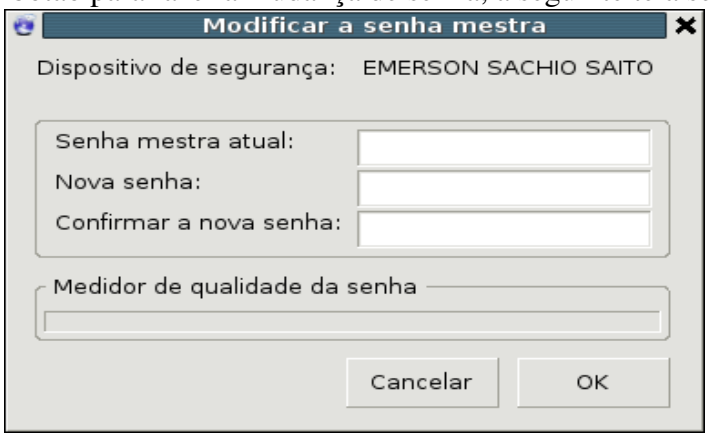

Figura 23 – Modificar a senha PIN.

Informe então a senha PIN onde está escrito “Senha mestra atual” e em seguida a Nova senha e a Confirmação da Senha.

7 CONSIDERAÇÕES FINAIS.

A homologação deste manual foi feita com o uso de uma leitora homologada pela ICP-BRASIL através o LEA – Laboratório de Ensaios e Auditoria (http://www.lea.gov.br/) mas as instruções devem funcionar para os dispositivos suportados pelo OPENCT (http://www.opensc-project.org/openct/).

A configuração do navegador Mozilla (http://www.mozilla.org), também é parecida com a apresentada e funciona da mesma forma, somente os itens de menus e telas é que estão em disposições diferentes. Não será apresentado neste manual pois não é o navegador padrão da CELEPAR, mas está homologado e funciona perfeitamente.

Para obter mais informações a respeito do funcionamento do Mozilla-Firefox entrar no site: http://www.mozilla.com/firefox/.

O Centro de Difusão de Tecnologia e Conhecimento (CDTC) do Governo Federal (http://cdtc.org.br/brasil/) oferece um curso para uso do Mozilla-Firefox.