



**PLATAFORMA DE DESENVOLVIMENTO PINHÃO PARANÁ**

**MANUAL DE CONFIGURAÇÃO DO CLIENTE DE E-MAIL MOZILLA  
THUNDERBIRD E COMPATÍVEIS**



**Agosto – 2006**

## Sumário de Informações do Documento

**Tipo do Documento:** Manual

**Título do Documento:** Manual de configuração do Mozilla Thunderbird

**Estado do Documento:** EB (Elaboração)

**Responsáveis:** Emerson Sachio Saito

**Palavras-Chaves:** Leitor, Smart, Card, Perto, USB, Certificado, Digital, Thunderbird

**Resumo:** Manual de configuração do leitor de e-mail Mozilla Thunderbird em ambiente LINUX/DEBIAN

**Número de páginas:** 22

**Software utilizados:** OpenOffice Writer

Versão	Data	Mudanças
--------	------	----------

1.0	30/08/2006	Criação ( Revisão: Cíntia A Evangelista )
-----	------------	---

1.1	06/02/2007	Mudança na URL da Raiz da ICP-BRASIL
-----	------------	--------------------------------------

# SUMÁRIO

<b>1 INTRODUÇÃO.....</b>	<b>4</b>
<b>2 PRÉ-REQUISITOS BÁSICOS.....</b>	<b>4</b>
<b>3 INSTALAÇÃO E CONFIGURAÇÃO DO MOZILLA THUNDERBIRD.....</b>	<b>5</b>
<b>4 CONFIGURAÇÃO DAS AUTORIDADES CERTIFICADORAS.....</b>	<b>8</b>
4.1 CONFIGURAÇÃO DAS LISTAS DE CERTIFICADOS REVOGADOS.....	11
<b>5 PROCEDIMENTOS.....</b>	<b>13</b>
5.1 CONFIGURAÇÃO DO CERTIFICADO EM ARQUIVO.....	13
5.2 CERTIFICADOS EM HARDWARE.....	14
5.2.1 <i>Pré-requisitos</i> .....	14
5.2.2 <i>Configuração e Ativação</i> .....	14
5.3 ENVIO DE MENSAGENS ASSINADAS E CRIPTOGRAFADAS. ....	16
5.4 VALIDAÇÃO DE ASSINATURA E RECEBIMENTO DE MENSAGENS CRIPTOGRAFADAS. ....	18
5.5 ALTERAÇÃO DE SENHA DE CERTIFICADO ARMAZENADO EM UM TOKEN OU SMARTCARD.....	20
<b>6 ADICIONANDO CERTIFICADOS (CHAVES PÚBLICAS) DOS CONTATOS.....</b>	<b>21</b>
<b>7 CONSIDERAÇÕES FINAIS.....</b>	<b>22</b>

## 1 INTRODUÇÃO

Este manual tem por objetivo orientar a configuração do leitor/cliente de E-MAIL Mozilla/Thunderbird e compatíveis para uso de certificados digitais em ambiente LINUX/DEBIAN. Isto fornece os meios para envio de e-mail criptografados e/ou com assinatura digital.

Será abordado o uso de certificados digitais armazenados em arquivos, que são os de nível A1 e S1, e 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 a aquisição destes conhecimentos.
- Cliente/Leitor de e-mail Mozilla/Thunderbird 1.5.0.4 ou superior.
- Instalação do pacote mozilla-psm que é o pacote de gerenciamento de segurança pessoal, que na maioria dos casos está na instalação padrão.
- Certificados padrão ICP-BRASIL.
- Cadeias de certificados da autoridade emissora e seus respectivos emissores e principalmente a cadeia RAIZ da IPC-BRASIL.

### 3 INSTALAÇÃO E CONFIGURAÇÃO DO MOZILLA THUNDERBIRD.

A grande maioria das instalações de LINUX já trazem este cliente de e-mail como padrão, por isto deve-se verificar se o mesmo já está instalado (menu: *Aplicações/Internet/Cliente de E-mail Thunderbird*).

Caso seja necessário a instalação é preciso permissão de root, e poderá ser feita através do comando ***apt-get install mozilla-thunderbird*** na console, ou pela interface gráfica synaptic que é a mais amigável e recomendada (veja figura 1).

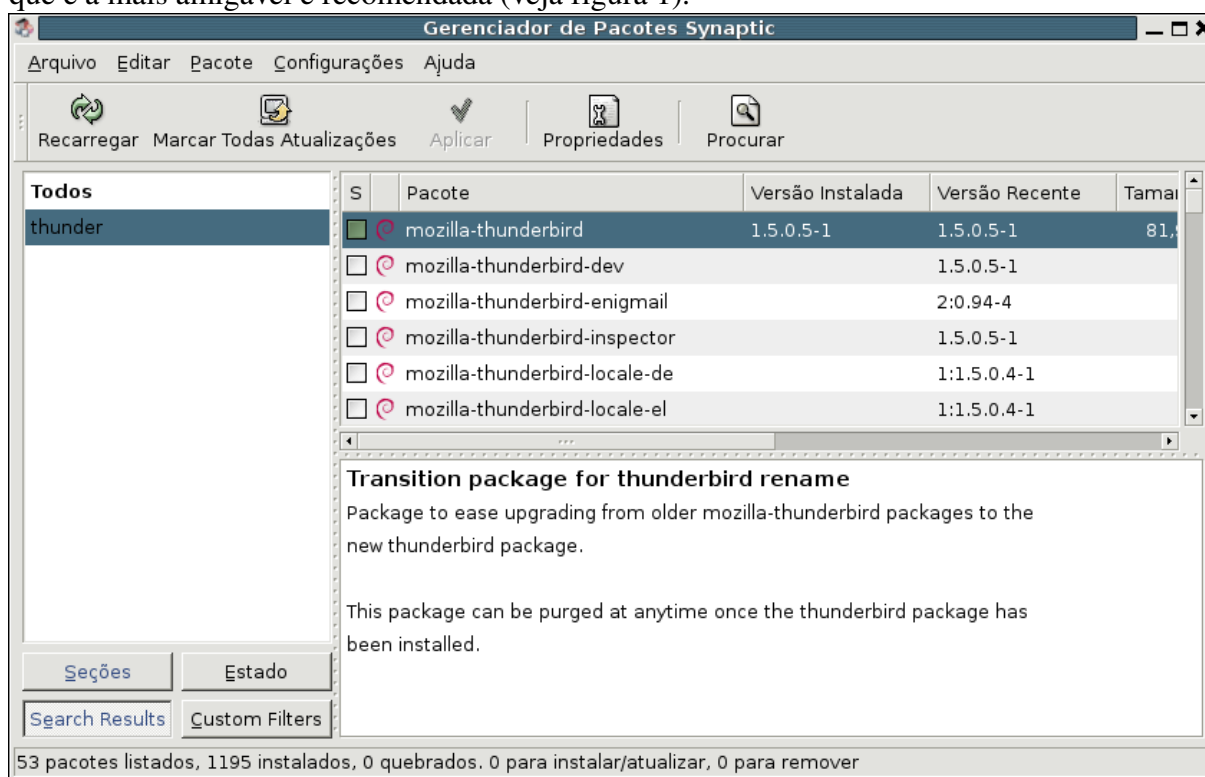


Figura 1 – Gerenciador de Pacotes Synaptic.

Com o programa instalado é preciso fazer as configurações da conta a ser acessada.

Executar o programa através do menu: *Aplicações/Internet/Cliente de E-mail Thunderbird*.

As telas seguintes serão apresentadas automaticamente:

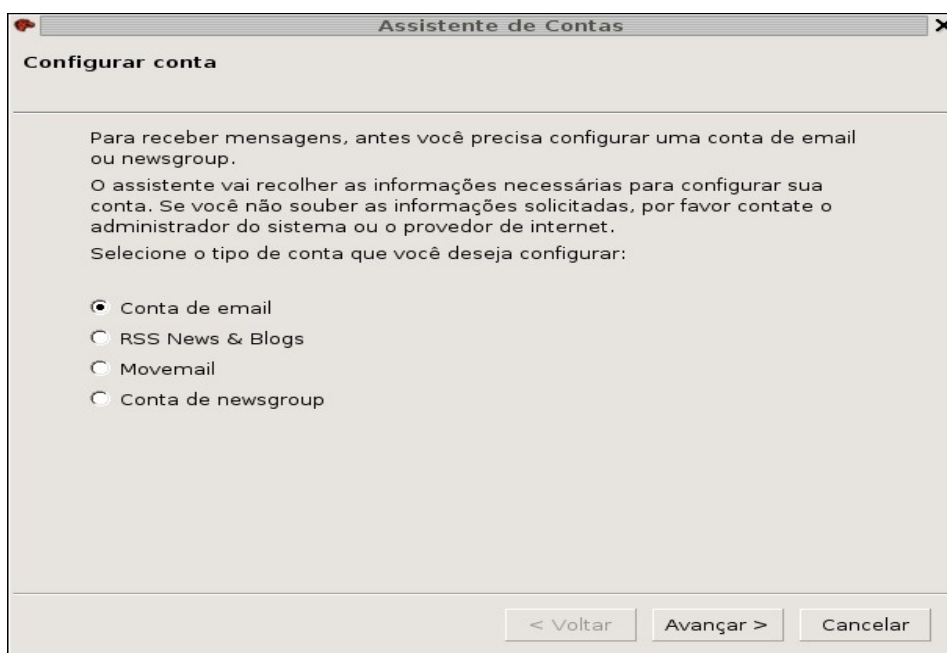


Figura 2 -Configurar conta

O primeiro passo será escolher Conta de email.

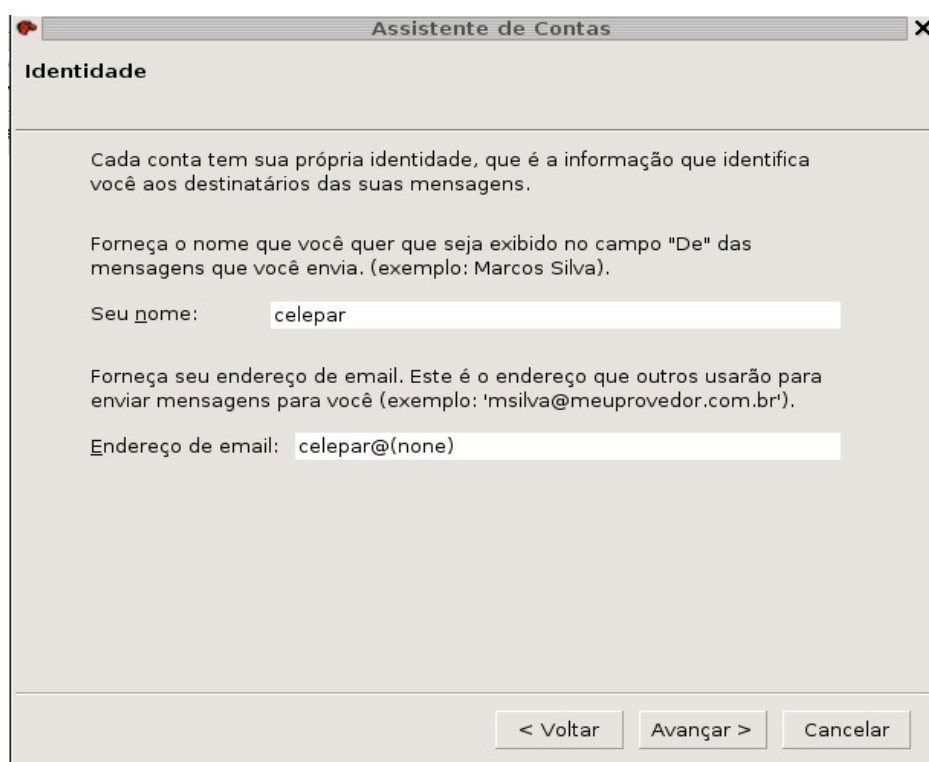
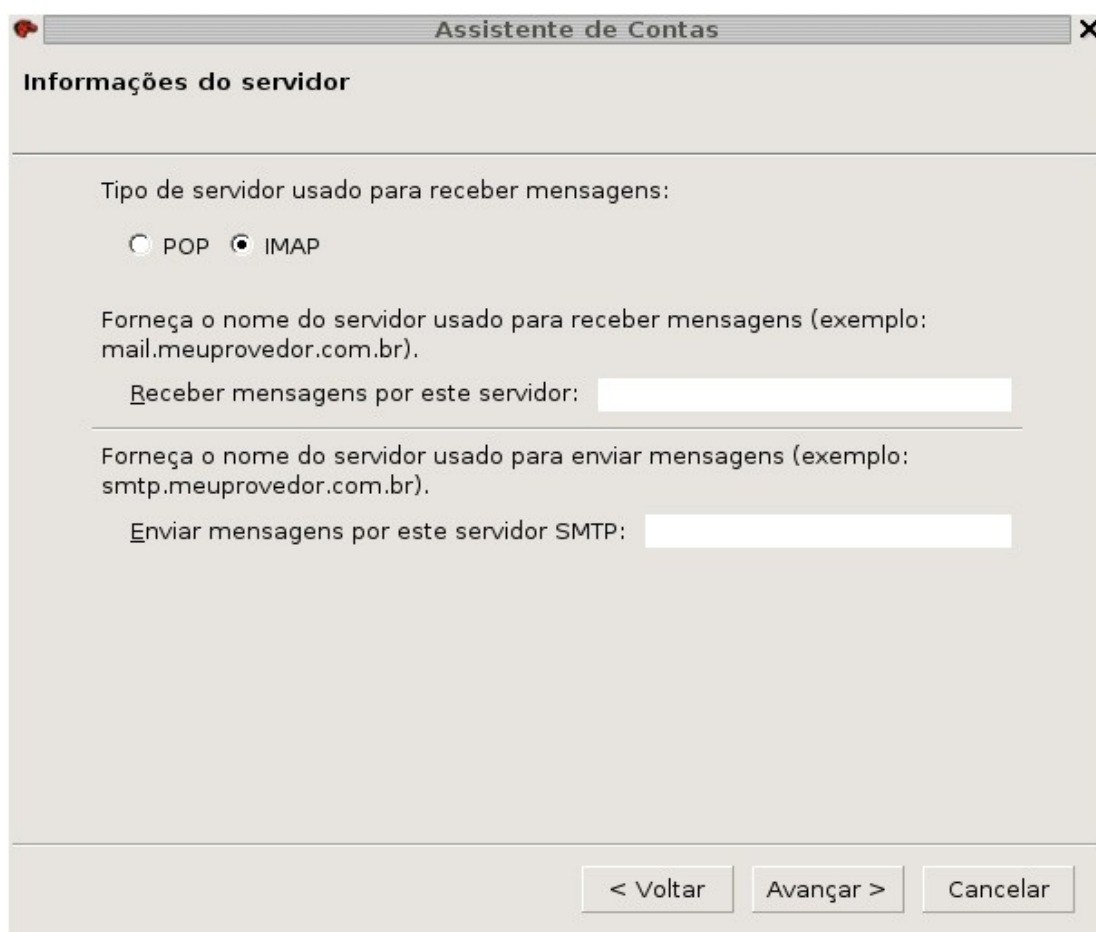


Figura 3 – Identidade

Informar o nome e o e-mail (para usuários da CELEPAR o e-mail do expresso).



A screenshot of a Windows-style dialog box titled "Assistente de Contas" (Account Assistant). The dialog has a standard title bar with a red icon, the title, and a close button (X). The main content area is titled "Informações do servidor" (Server Information). It contains the following elements: a label "Tipo de servidor usado para receber mensagens:" followed by two radio buttons, "POP" and "IMAP", with "IMAP" selected; a text label "Forneça o nome do servidor usado para receber mensagens (exemplo: mail.meuprovedor.com.br)."; a text input field labeled "Receber mensagens por este servidor:"; another text label "Forneça o nome do servidor usado para enviar mensagens (exemplo: smtp.meuprovedor.com.br)."; and a text input field labeled "Enviar mensagens por este servidor SMTP:". At the bottom right, there are three buttons: "< Voltar" (Back), "Avançar >" (Next), and "Cancelar" (Cancel).

Figura 4 – Informações do Servidor.

Nesta tela informar o tipo do servidor, que no caso dos usuários da CELEPAR é o IMAP, e também os endereços para Receber e Enviar que no caso da CELEPAR é o **expressomx.pr.gov.br** para ambos.

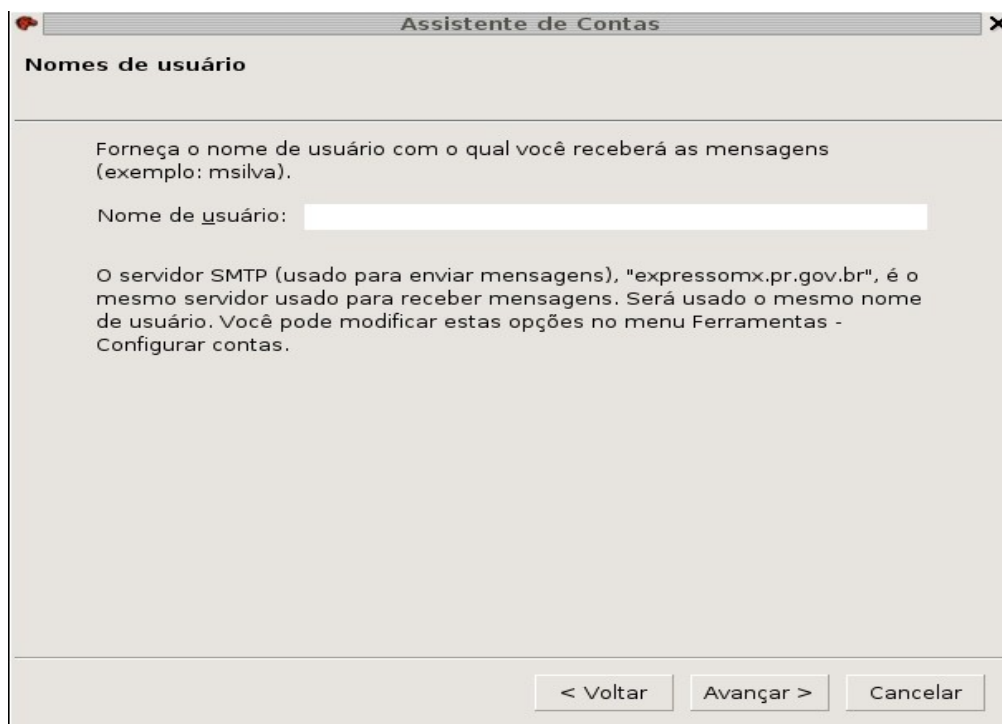


Figura 5 -Nome de usuário.

Informar o usuário no servidor de e-mail, para usuários da CELEPAR o padrão é CELEPAR-<nome>. Para outros usuários do expresso é <ORGÃO>-<nome>.

Na sequência será apresentada uma tela de confirmação das configurações básicas.

#### 4 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.

Certificar-se que os arquivos(.cer) dos certificados das autoridades, estejam em um diretório acessível.



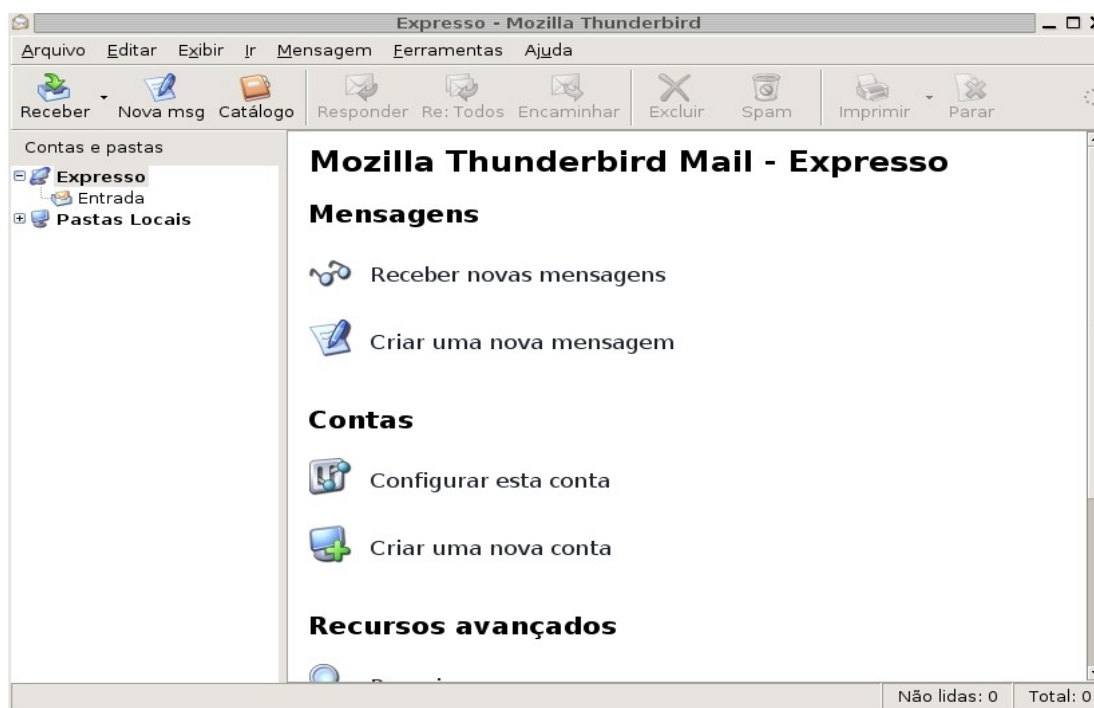


Figura 6 – Tela principal do Thunderbird.

Com o Thunderbird aberto selecionar a conta (no painel à esquerda) que será configurada, clicar com botão direito do mouse, escolher a opção **propriedades** ou via menu **Editar/Configurar Contas...** logo a tela abaixo aparecerá:

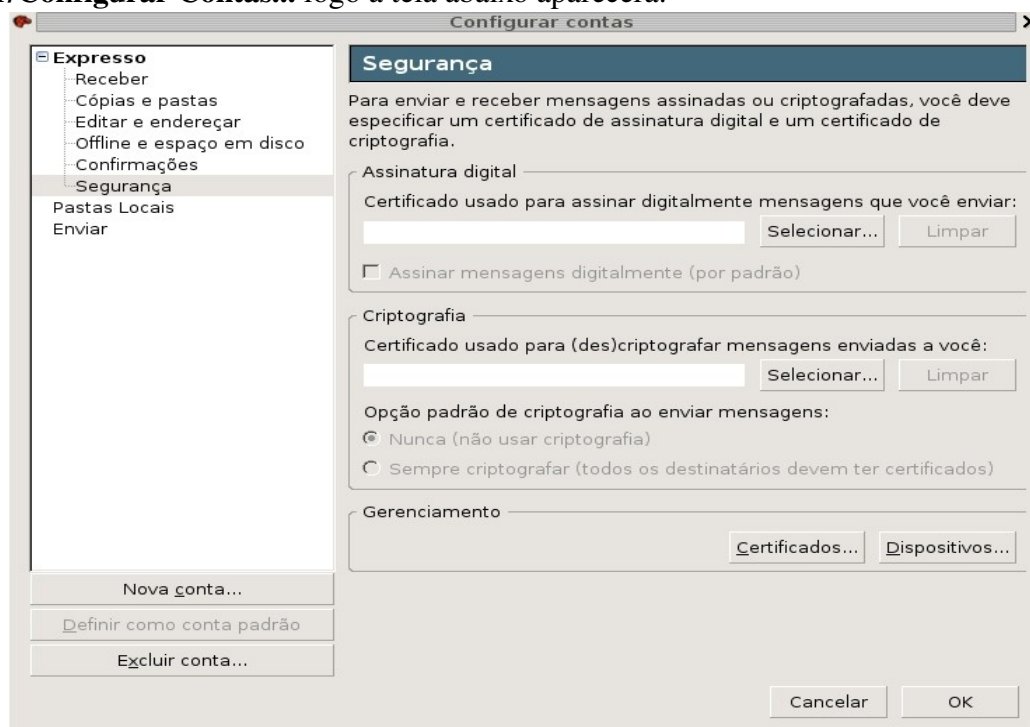


Figura 7 – Configurar contas.

Selecionar a opção segurança conforme a figura 7, em seguida clicar no botão **Certificados** no quadro Gerenciamento.

Na tela apresentada clique na aba **Autoridades**

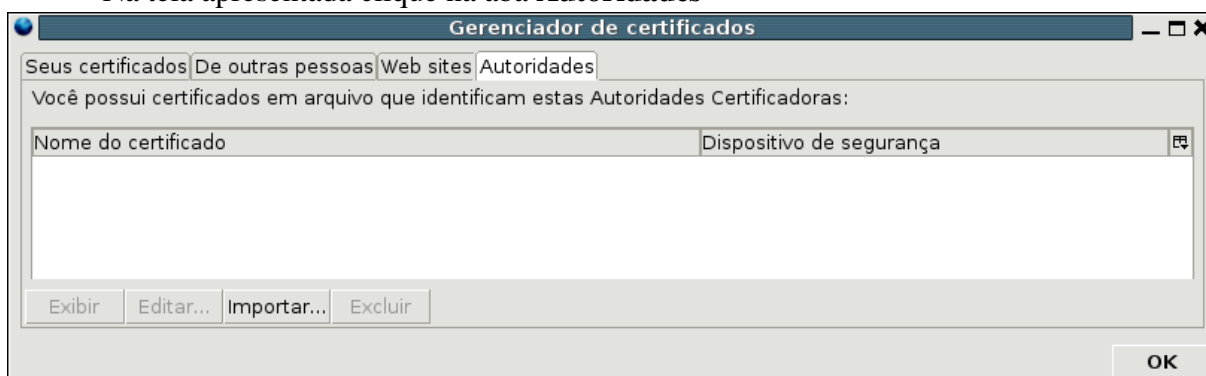


Figura 8 – Gerenciador de certificados na aba autoridades.

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

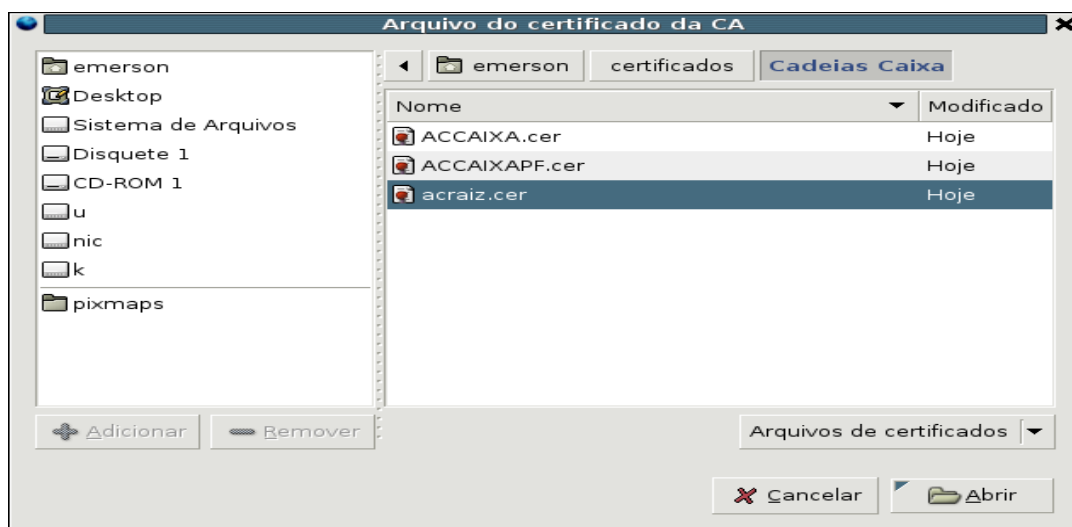


Figura 9 – Arquivos de certificados.

Será necessário repetir a tarefa para cada arquivo conforme a hierarquia, partindo da RAIZ da ICP-BRASIL que é obrigatório, e depois as demais conforme a hierarquia, e marcar todas as opções de confiança e finalidades conforme a tela abaixo:

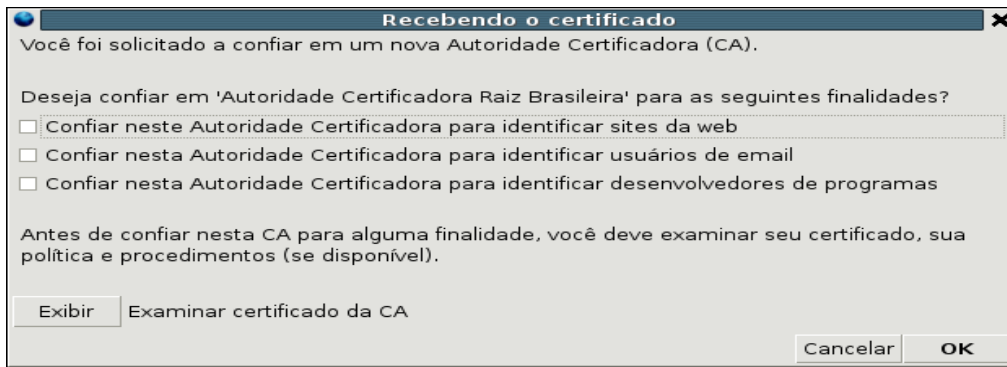


Figura 10 – Recebendo o certificado.

Esta tarefa é necessária para a inclusão dos certificados autênticos.

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

#### 4.1 Configuração das Listas de Certificados Revogados.

O complemento para configuração das autoridades é a inclusão das listas de revogações, que garante a validade dos certificados.

Para configurá-lo é preciso abrir a tela de preferências no menu: Editar/Preferências (alt+e+n). Abrirá a tela de preferências do Thunderbird:



Figura 11 – Preferências.

Clicar no ícone **Privacidade** e em seguida na aba **Segurança** (figura 11), clicar então no botão **Revogações** que apresentará a tela abaixo:



Figura 12 – Gerenciador de CRL (lista de certificados revogados)

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

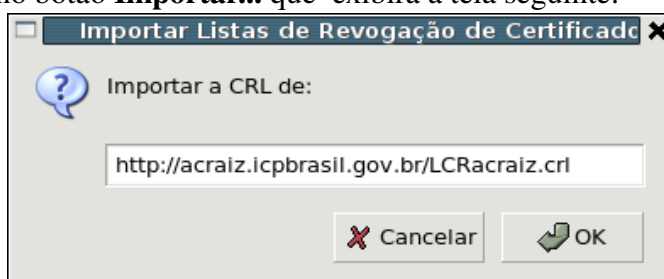


Figura 13 – Importar Listas de Revogação de Certificado

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 procedimento para todas as autoridades certificadoras, conforme a hierarquia do certificado que está sendo utilizado.

## 5 PROCEDIMENTOS

### 5.1 Configuração do certificado em arquivo.

Repetir os passos do item anterior até a figura 8.

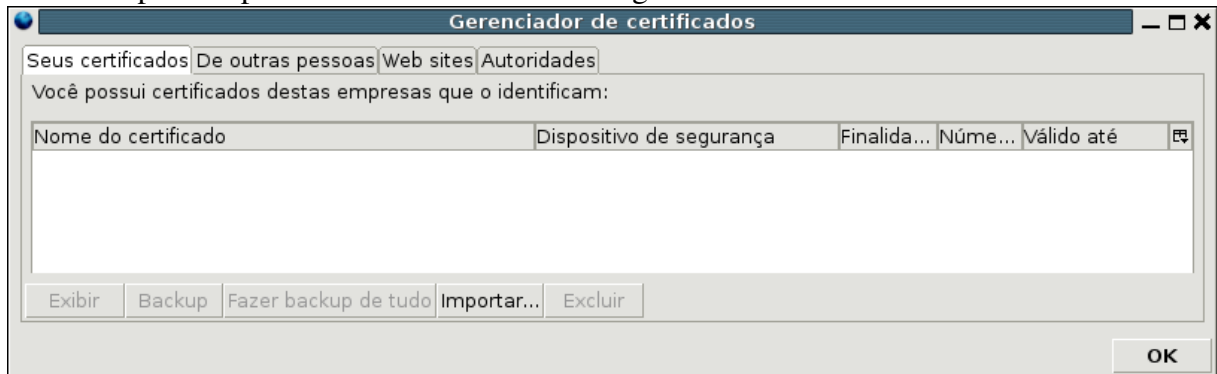


Figura 14 – Gerenciador de certificados – Destaque para Seus certificados.

Depois clicar no botão **Importar...** e informar o diretório e o nome do arquivo de certificado no formato PKCS12 (.pfx ou .p12).

Neste momento o programa pedirá a senha MESTRE para os dispositivos de segurança, esta senha servirá para que o Thunderbird utilize os certificados. Em seguida será pedida a senha para o certificado e a tela de confirmação aparecerá.

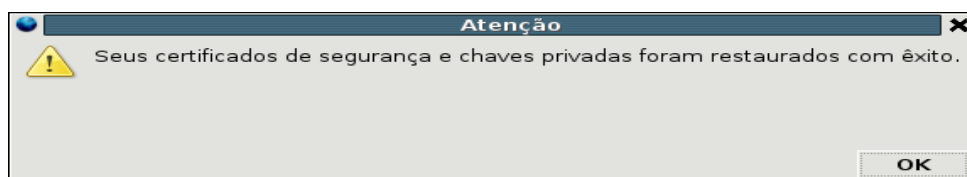


Figura 15 – Confirmação de importação.

Após isto o certificado deverá ser listado na tela da figura 11.

A partir deste momento o certificado estará armazenado no Thunderbird e a senha para uso é a mesma que foi informada como senha MESTRE.

No item 5.3 será demonstrado como fazer assinatura e cifragem de mensagens.

## 5.2 Certificados em hardware

O Thunderbird também foi desenvolvido para trabalhar com certificados armazenados em hardware, que são os Tokens e SmartCards (níveis A2,A3, A4, S2,S3 e S4) neste item será feita a configuração destes dispositivos.

### 5.2.1 Pré-requisitos

- Instalação e configuração da leitora de SmartCard ou Token: ver arquivo **GIC\_ManualInstalacaoLeitorSmartCard**.
- Configuração das Autoridades Certificadoras conforme o item 4 deste manual.

### 5.2.2 Configuração e Ativação.

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.

Seguir o item 4 até a figura 7.

Na aba Gerenciamento clicar no botão **Dispositivos...** que mostrará a tela abaixo:

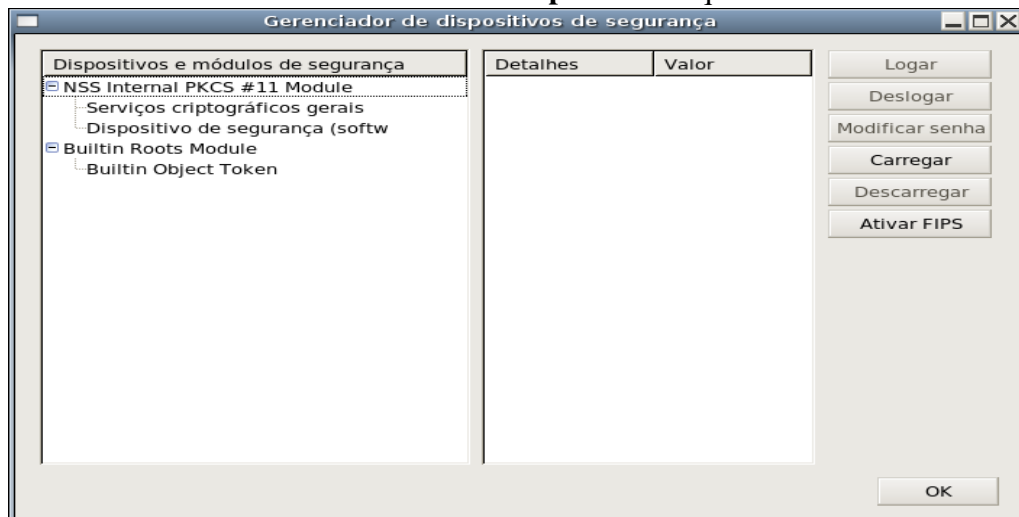


Figura 16 – Gerenciador de dispositivos de segurança.

Clicar no botão **carregar** que abrirá a tela abaixo:

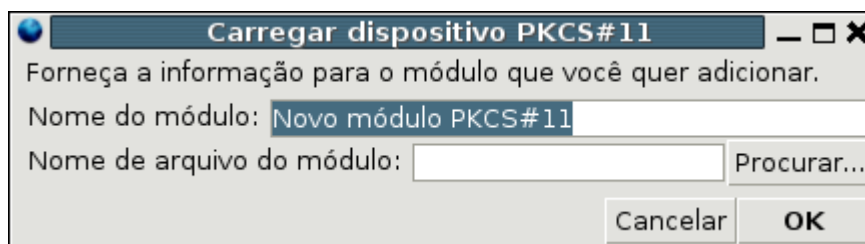


Figura 17 – Carregar dispositivo PKCS#11

Nesta tela informar o **Nome do módulo**, que poderá ser qualquer nome de fácil identificação, como por exemplo: “Leitora SmartCard”, 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), esta forma é a mais prática e também para casos onde o arquivo *opensc-pkcs11.so* não esteja no diretório /usr/lib/opensc.

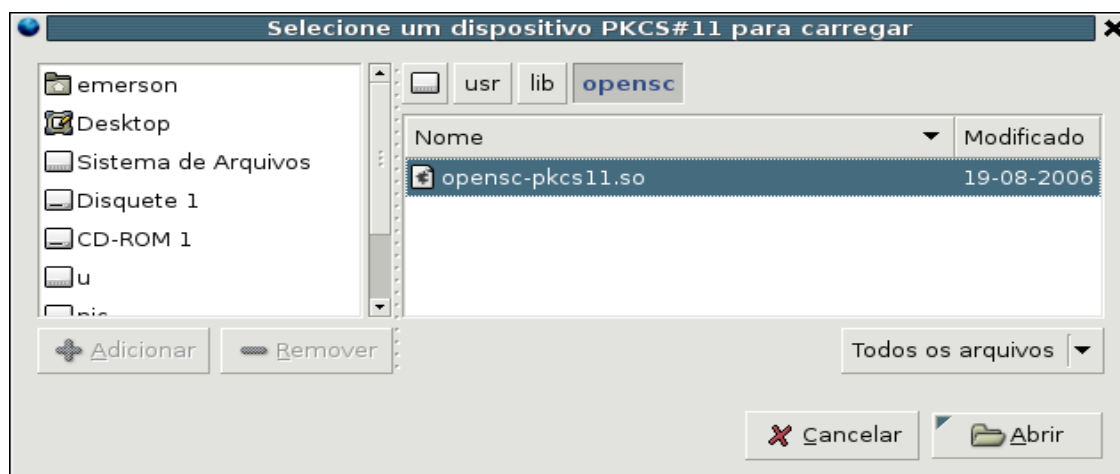


Figura 18 – Seleção do dispositivo de segurança.

Logo após será apresentada a tela abaixo:

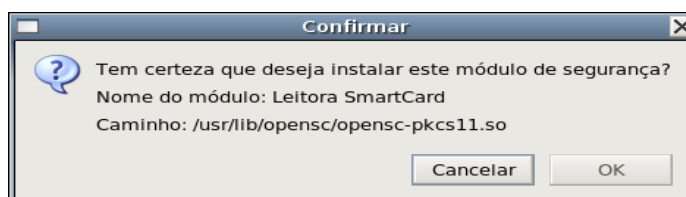


Figura 19 – Confirmação para instalar módulo

Neste momento o certificado será lido e carregado, o que poderá levar um certo tempo dependendo do equipamento.

Após isto o certificado deverá ser listado como na figura abaixo:

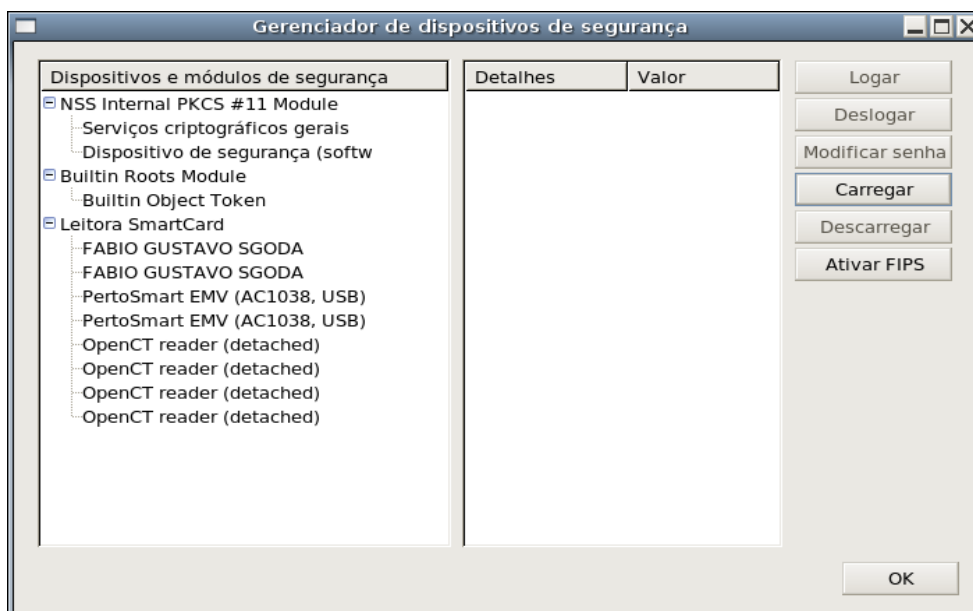


Figura 20 - Gerenciador de Dispositivos de Segurança – À esquerda o novo dispositivo.

Assim o Thunderbird estará apto a ler o certificado digital armazenado na Leitora ou Token.

### 5.3 Envio de mensagens Assinadas e Criptografadas.

Nos itens anteriores foi orientada a instalação e configuração dos certificados digitais, tanto para armazenamento em arquivo como para hardware. Para a execução das tarefas de Assinatura e Criptografia a configuração é a mesma para ambos e o Thunderbird irá tratá-los da mesma forma.

Seguir o item 4 até a figura 7.

Nesta tela tanto para o quadro **Assinatura Digital** e **Criptografia** pode-se selecionar o certificado que será usado para estas tarefas, para isto deve-se clicar no botão **Selecionar...** que apresentará a tela abaixo onde será listado o certificado que foi incluído.



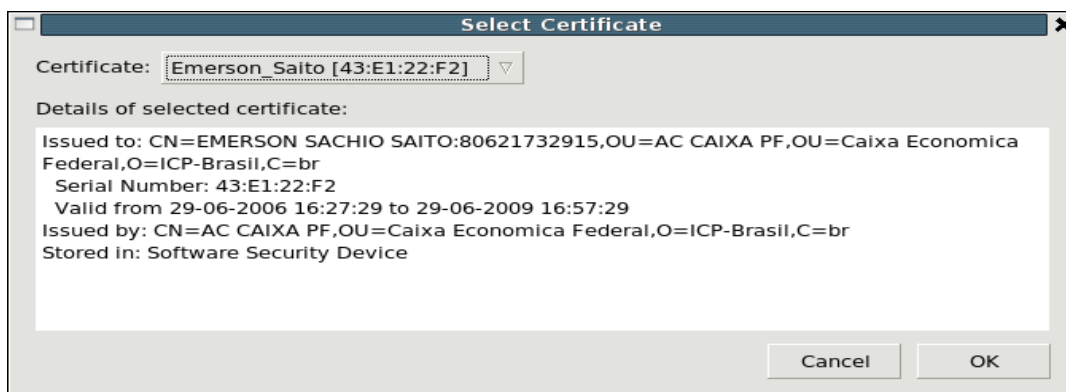


Figura 21 – Seleção do certificado para Assinatura Digital e Criptografia.

Para certificados em arquivos é obrigatório executar este passo para o quadro **Criptografia**.

No caso de certificados em hardware (SmartCard ou Token) o Thunderbird apresentará a seguinte tela:

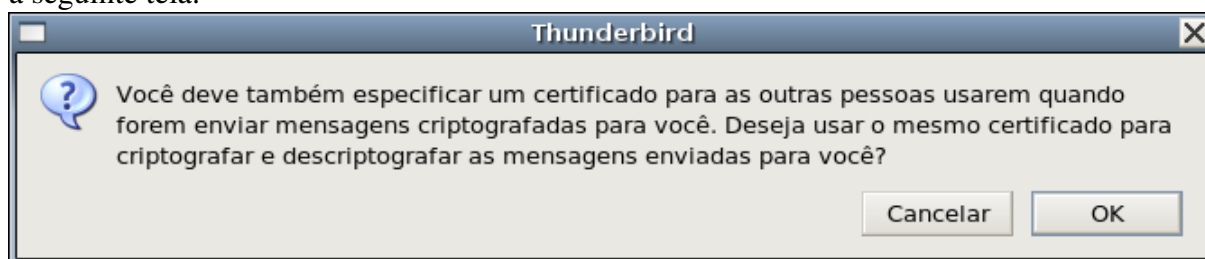


Figura 22 – Certificado para criptografia.

Clicar no botão OK para que o certificado de criptografia seja selecionado automaticamente, clicar em CANCELAR somente se estiver utilizando certificados diferentes para Assinatura e Criptografia.

Com estes procedimentos o Thunderbird estará preparado para assinar e criptografar as mensagens.

Para criptografar mensagens é necessário ter armazenado a chave pública dos contatos, e a forma mais fácil e automática para isto, é pedir aos contatos para enviarem uma mensagem assinada digitalmente, a partir do momento que o Thunderbird ler esta mensagem, ele irá armazenar a chave pública do contato.

Também é importante enviar a própria assinatura para os contatos, para que estes possam reenviar mensagens criptografadas.

Para se verificar as chaves dos contatos deve-se seguir o item 4 até a figura 8.

Na tela apresentada clicar na aba **De Outras Pessoas**, que listará todas as chaves públicas armazenadas, estes serão os contatos para os quais poder-se-á criptografar uma mensagem.

Para assinar uma mensagem basta criar uma nova mensagem e seleccionar no menu **Opções/Segurança/Assinar Digitalmente.**

Para criptografar uma mensagem selecione no menu **Opções/Segurança/Criptografar**, lembrando que a criptografia é somente para os contatos com chaves públicas.

Também é possível assinar e criptografar a mesma mensagem.

#### **5.4 Validação de Assinatura e recebimento de mensagens criptografadas.**

Ao receber uma mensagem a mesma pode estar: assinada, criptografada ou com ambas as opções.

As mensagens criptografadas só poderão ser abertas pelo receptor, se o emissor utilizou a chave pública do certificado que o receptor está utilizando, neste caso o Thunderbird só poderá apresentá-las se o certificado do receptor estiver armazenado e configurado, no caso dos Tokens e SmartCards, se os mesmo estiverem disponíveis. Ao abrir a mensagem o Thunderbird pedirá a senha do certificado ou a senha mestre, no caso dos certificados em arquivos. A senha é pedida apenas uma vez por sessão/abertura do programa, ou caso o Token ou SmartCard for desconectado.

A validação de assinatura é uma tarefa bem simples: ao receber a mensagem, esta apresentará um ítem a mais, que é a assinatura do emissor apresentado como o ícone abaixo:



Veja a tela de uma mensagem assinada:



Figura 23 – Mensagem assinada.

Para verificar a assinatura, posicionar a seta do mouse no ícone apresentado acima e clicar duas vezes com o botão direito, o Thunderbird deverá apresentar a tela abaixo com as informações da assinatura:

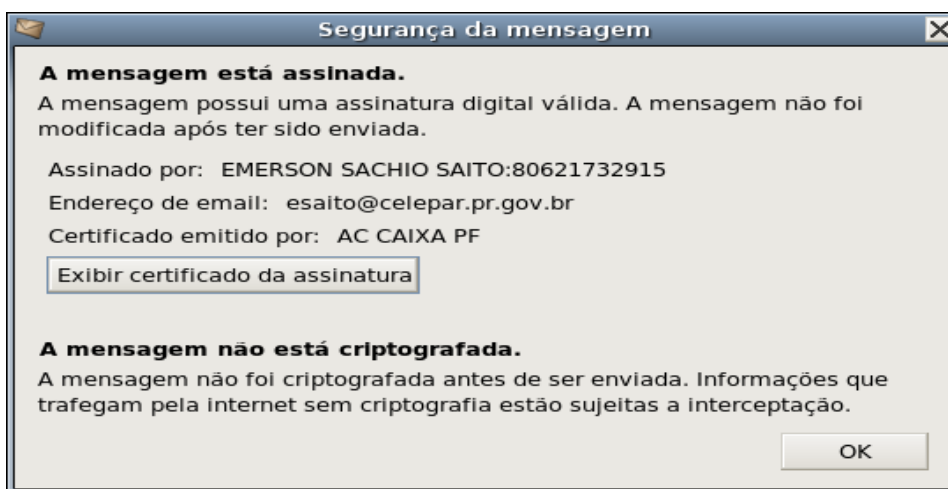


Figura 24- Assinatura da Mensagem.

A tela apresenta que a mensagem possui uma assinatura válida e garante que a mensagem não foi corrompida.

## 5.5 Alteração de senha de Certificado Armazenado em um Token ou SmartCard.

Através do Thunderbird é possível alterar, caso desejado, a senha do certificado armazenado no Token ou SmartCard, para isto selecionar o menu Editar/Preferências que apresentará a tela abaixo:

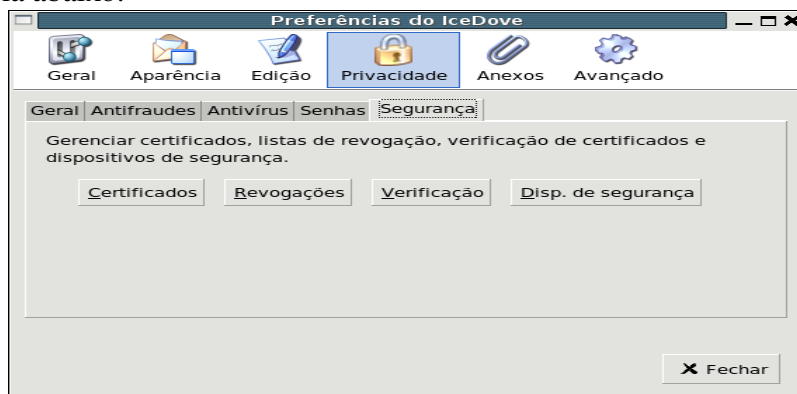


Figura 25- Tela de Preferências.

Clicar no ícone **Privacidade**, depois na aba **Segurança**, em seguida em Disp. de Segurança. A tela abaixo deverá aparecer.



Figura 26- Assinatura da Mensagem.

Selecionando o Certificado no dispositivo (normalmente apresenta o nome do proprietário) será habilitado o botão **Modificar senha**. Deve-se clicar neste botão para que se possa fazer a mudança de acordo com o desejado, conforme mostrado na figura abaixo:

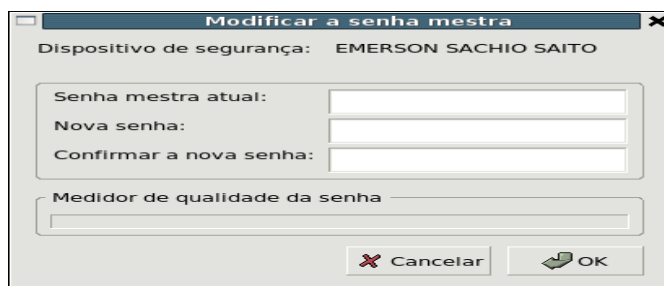


Figura 27- Mudança de senha do certificado.

## 6 ADICIONANDO CERTIFICADOS (CHAVES PÚBLICAS) DOS CONTATOS.

O Thunderbird faz o armazenamento automático dos certificados (chaves públicas), dos contatos que enviaram uma mensagem assinada. O e-mail do certificado deverá corresponder ao endereço de e-mail utilizado para enviar a mensagem.

Em outros casos talvez seja necessário, adicionar manualmente um certificado para um endereço de e-mail.

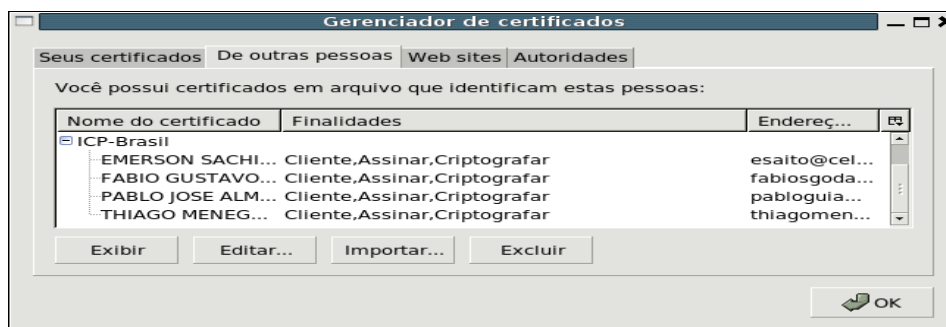
Utilize o menu Editar/Preferências. Que irá exibir a seguinte tela:



Figura 28- Preferências

A partir desta tela clicar no botão Certificados que mostrará a tela abaixo:

Figura 29- Gerenciador de Certificados.



Clicar então no botão importar e indicar o arquivo do certificado de chave pública, que deverá ser importado (normalmente com as extensões .pem ou .cer).

## 7 CONSIDERAÇÕES FINAIS.

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

Para se obter mais informações a respeito do funcionamento do Mozilla-Thunderbird, entrar no site: <http://www.mozilla.com/thunderbird/>.

O Centro de Difusão de Tecnologia e Conhecimento (CDTC) do Governo Federal (<http://cdtc.org.br/brasil/>), oferece um curso para uso desta ferramenta.

Existe uma lista sobre perguntas freqüentes, que auxiliam no uso de certificados digitais no documento: GIC\_ManualUsuarioCertificacaoDigital.

No ambiente DEBIAN, por questões de licenciamento, o leitor é o ICEDOVE que na realidade é o mesmo Thunderbird.