

# PLATAFORMA DE DESENVOLVIMENTO PINHÃO PARANÁ MANUAL DO USUÁRIO PARA O CRYPTONIT



Sumário de Informações do Documento			
		,	
Tipo do Documento: Manual			
Título do Documento: MANUAL DO USUÁRIO PARA CRYPTONIT			
Estado do Documento: EB (Elaboração)			
Responsáveis: Emerson Sachio Saito			
Palavras-Chaves: Certificação, Digital, Cryptonit, Assinatura, Criptografia			
Resumo: Manual do usuário para o software Cryptonit que permite facilidades de certificação digital			
Número de páginas: 25			
Software utilizados: OpenOffice Writer			
Versão	Data	Mudanças	
1.0	21/08/2006	Criação ( Revisão: Cíntia A Evangelista)	

# **SUMÁRIO**

1 APRESENTAÇÃO	4
1.2 Finalidade de Uso do Software	∠
2 USANDO O SOFTWARE	5
2.1 Instalação.	
2.2 Utilizando a ferramenta.	<i>6</i>
2.2.1 Pré-requisitos	6
2.2.2 Tela inicial	6
2.2.3 Configurações	
2.2.3.1 Incluir cadeias de certificados (AUTORIDADES)	
2.2.3.2 Incluir certificado (IDENTIDADES)	11
2.2.3.2.1 Incluir identidade para certificado armazenado em arquivo	12
2.2.3.3 Dispositivos	14
2.2.3.4 Outras configurações	
2.2.4 Adicionar Contatos	16
2.2.5 Preparação de arquivos	
2.2.6 Codificar/Criptografar arquivos	19
2.2.7 Decodificar arquivos	
2.2.8 Assinatura de arquivos.	22
2.2.9 Verificação de Assinatura	24
3 CONSIDERAÇÕES FINAIS	25

## 1 APRESENTAÇÃO

Em várias situações, é necessário o uso de um software para efetuar assinaturas em arquivos não estruturados (imagem, som, vídeo) e os mesmos não estão armazenados em nenhum sistema, ou ainda necessitam de um processo ágil e fácil de assinatura (como por exemplo em processos de digitalização).

Para estes casos existem algumas alternativas, muitas delas proprietárias, e uma das que se mostram bastante eficiente e também por ser uma alternativa livre foi o software Cryptonit, para o qual foi confeccionado este manual de uso.

#### 1.2 Finalidade de Uso do Software

O software Cryptonit (<a href="http://sourceforge.net/projects/cryptonit">http://www.cryptonit.org</a>) é um projeto Open Source e sob licença GPL, que foi identificado como uma boa opção, para uso em tarefas de Assinatura e Criptografia com certificados digitais no ambiente Desktop. É muito semelhante em uso e funções a vários produtos comercializados pelo mercado, com a vantagem de ser código aberto e executável tanto em ambiente operacional livre como proprietário.

Neste documento será apresentado um manual de referência para usuário final e está baseado no uso em ambiente operacional LINUX/DEBIAN, provavelmente deverá ter o mesmo comportamento em ambiente proprietário. Também está sendo considerado o padrão ICP-BRASIL para certificação digital.

Recomenda-se que o usuário deste manual tenha conhecimentos prévios de certificação digital, pois muitos termos utilizados neste documento não serão explicados com os devidos detalhes. Estes conhecimentos podem ser adquiridos através do curso e material fornecidos pela GIC e é parte integrante da Plataforma de Desenvolvimento PINHÃO PARANÁ.

#### 2 USANDO O SOFTWARE

#### 2.1 Instalação

Para fazer a instalação do software basta executar o comando "apt-get install cryptonit," em um terminal com permissão de root ou utilizar a interface gráfica "synaptic", que é o meio mais amigável e recomendado para o usuário final.

Todas as dependências exigidas deverão ser instaladas, em alguns casos pode ser que já

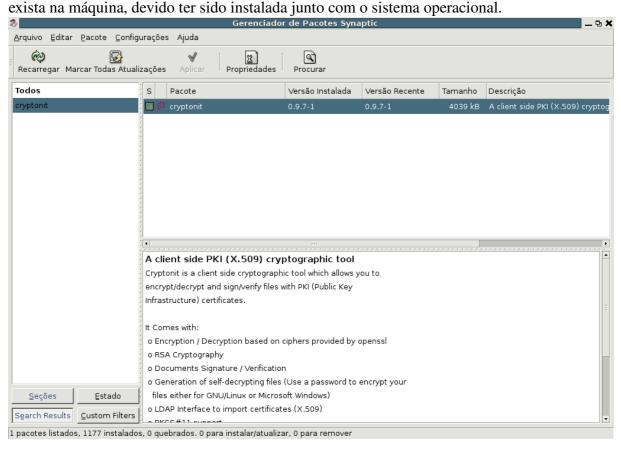


Figura 1. Tela do Synaptic com o pacote cryptonit em destaque.

#### 2.2 Utilizando a ferramenta.

#### 2.2.1 Pré-requisitos.

De acordo com padrões pré-definidos serão necessárias as cadeias de certificado da AC-RAIZ da ICP-BRASIL e das AC's (Autoridade Certificadora), credenciadas de acordo com o certificado a ser utilizado, que preferencialmente deverá ser padrão ICP-BRASIL.

Será necessário providenciar estas cadeias, que podem ser obtidas na página internet da AC que emitiu o certificado e em muitos casos são entregues juntamente com o certificado. Deve-se armazenar estas cadeias em um diretório temporário e no qual se tenha acesso (veja item 2.2.3.4 -Diretório).

O certificado da IPC-BRASIL é encontrado em: <a href="http://www.icpbrasil.gov.br/">http://www.icpbrasil.gov.br/</a>.

#### 2.2.2 Tela inicial

Ao iniciar a ferramenta (linha de comando: **cryptonit**) pelo menu **Aplicações/Ferramentas de Sistema/Cryptonit**), a seguinte tela será apresentada:



Figura 2. Tela inicial

#### 2.2.3 Configurações

A primeira tarefa a ser executada para possibilitar o uso da ferramenta, é fazer a sua configuração para isto é preciso seguir os seguintes passos:

Clicar no botão "Configuração":





A seguinte tela será apresentada:

Figura 3. Propriedades configuráveis.

#### 2.2.3.1 Incluir cadeias de certificados (AUTORIDADES)

Ao lado esquerdo estão as opções configuráveis, a primeira configuração necessária é a das "Autoridades", que é a inclusão das cadeias das AC's, correspondentes ao certificado utilizado. É preciso adicionar estas cadeias, sendo que a AC RAIZ ICP-BRASIL, será a primeira e obrigatória conforme está definido como padrão.

Para isto selecionar a opção **Autoridades** no lado esquerdo da tela anterior, e em seguida, clicar no botão "adicionar um nova autoridade", conforme é apresentada na tela seguinte:

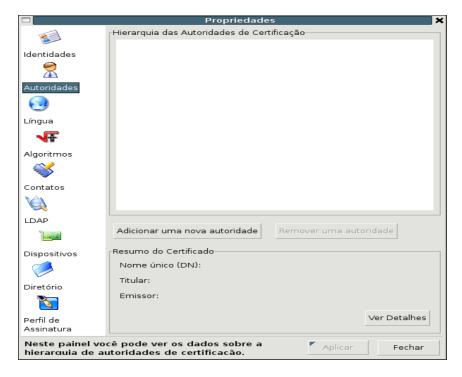


Figura 4. Configuração de Autoridades.

Na sequência informar o diretório e os arquivos (.cer), onde estão as cadeias dos certificados que se deseja inserir, lembrando sempre que a primeira é a cadeia da ICP-BRASIL RAIZ, caso esta já exista basta inserir as cadeias das outras AC's de nível 1 e subsequentes, que após executado o mesmo passo anterior para cada arquivo, deverão aparecer em uma estrutura hierárquica conforme mostrado na figura seguinte:

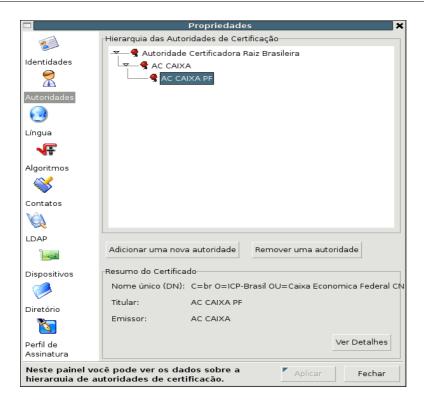
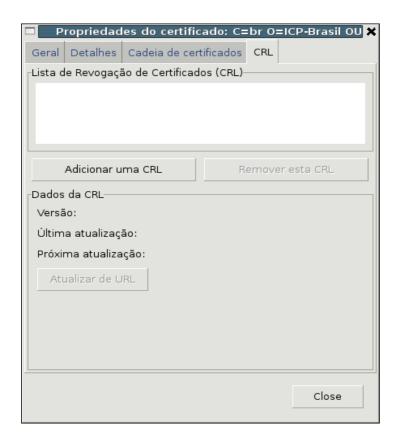


Figura 5. Listagem das cadeias inseridas.

Para excluir uma cadeia basta clicar no botão "Remover uma autoridade".

Clicando no botão "Ver Detalhes", para cada uma das autoridades listadas, é possível listar o conteúdo das cadeias e ainda possibilita a inclusão da Lista de Certificados Revogados (aba CRL). Esta lista poderá ser incluída através de três formas: de um arquivo que pode ser baixado do site da autoridade certificadora, informando o endereço(url) que consta no certificado, ou ainda utilizando um servidor LDAP.

Veja as figuras abaixo:



Figuras 6 – Selecionada a aba CRL (Lista de Revogação de Certificados)

Clicar no botão Adicionar uma CRL para visualizar a tela abaixo:

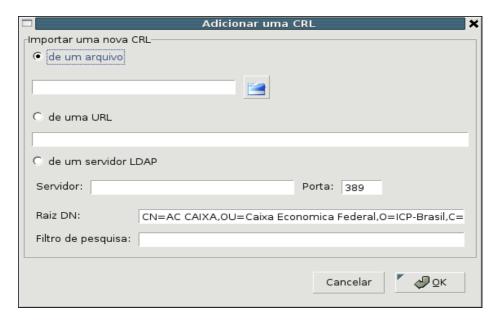


Figura 7 - Inclusão de Lista de Certificado Revogado.

11

A maneira mais cômoda caso possua uma conexão internet disponível, é informar a

URL, que é o endereço onde se encontra a lista de certificados revogados para cada

autoridade.

Selecionando a opção \*de uma URL:

Para a RAIZ da ICP-BRASIL é: <a href="http://acraiz.icpbrasil.gov.br/LCRacraiz.crl">http://acraiz.icpbrasil.gov.br/LCRacraiz.crl</a>

Para cada uma das outras AC's informar a url correspondente.

Neste exemplo:

AC Caixa: https://icp.caixa.gov.br/repositorio/ACCAIXA1.crl

AC Caixa PF: <a href="https://icp.caixa.gov.br/repositorio/ACCAIXAPF1.crl">https://icp.caixa.gov.br/repositorio/ACCAIXAPF1.crl</a>

Esta modalidade, desde que haja conexão internet, garante a atualização da lista.

No caso de uso com arquivos, partindo da figura 7, selecionar a opção \*de um arquivo

e clicar no ícone logo à frente, para informar o diretório e o arquivo (.crl) para cada

autoridade. Este tipo de configuração é a mais viável quando não há uma conexão com

internet, mas tem como desvantagem que a atualização também deverá ser feita manualmente,

conforme a política de atualização adotada pela empresa.

Para um servidor LDAP é necessário que haja um serviço deste tipo disponível no

ambiente que estiver usando, pois as configurações deverão ser informadas pelo administrador

do ambiente. Neste caso o administrador do LDAP é quem fará as atualizações das listas.

2.2.3.2 Incluir certificado (IDENTIDADES)

Com as autoridades configuradas é possível a inclusão de um certificado para

Assinatura e Criptografia, que é o certificado de uso pessoal, a obrigatoriedade para

configuração das autoridades é para o padrão ICP-BRASIL. Como existem duas formas de

armazenamento destes certificados, a explicação se fará por modalidade:

#### 2.2.3.2.1 Incluir identidade para certificado armazenado em arquivo.

Os certificados armazenados em arquivos são os de nível A1 e S1.

Para adicionar este tipo de certificado, deve-se selecionar a opção "Identidades" na tela de configurações (ver figura 3), e depois clicar no botão adicionar que fica ao lado direito da tela. Em seguida será apresentada a tela abaixo:

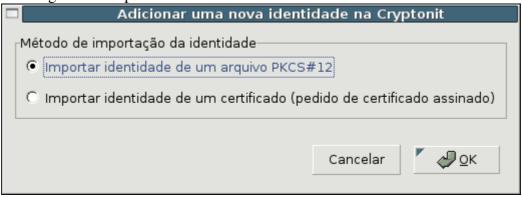


Figura 8. Importação do certificado.

Selecionar a primeira opção (Importar identidade de um arquivo PKCS#12) que apresentará a tela seguinte:

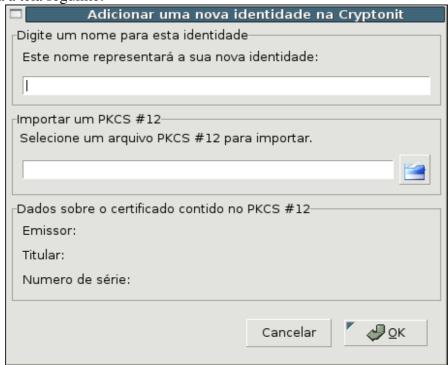


Figura 9. Importação de certificado.

Clicar no ícone azul para selecionar um arquivo PKCS#12 e indicar o diretório. Neste momento a senha (PIN) do certificado será requisitada:

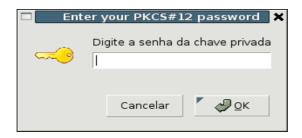


Figura 10. Senha do certificado.

Depois de informada a senha e retornado à tela da figura 9, deve-se informar o Nome do titular do certificado e confirmar (botão OK).

Caso a lista de certificados revogados não estiver disponível, a ferramenta apresentará um alerta , porém isto não é tecnicamente um impedimento ao uso da ferramenta.

Nas opções de "Identidades" existem as funcionalidades (botões) de:

- Remover o certificado, que excluirá um certificado importado.
- Ver detalhes, que listará o conteúdo.
- Exportar, que permite a exportação do certificado (restrita conforme o nível do certificado).
- Pedido de certificado, esta opção gera um arquivo que poderá ser enviado a uma
   Autoridade Certificadora (Não é permitido no padrão ICP-BRASIL).

#### 2.2.3.3 Dispositivos.

Para utilizar este recurso é necessário antes de tudo, fazer a instalação do dispositivo de leitura, que poderá ser um SmartCard ou Token, para isto deve-se utilizar o documento: GIC\_ManualInstalacaoLeitorSmartCard que também faz parte da plataforma PINHÃO.

Com o dispositivo instalado conforme o documento citado é possível continuar a configuração. Certificar-se de que o SmartCard esteja na leitora ou o Token plugado.

Para executar esta tarefa selecionar a opção "Identidades" na tela de configurações (ver figura 3) e depois clicar no botão carregar, o qual fica ao lado direito da tela (conforme figura abaixo).



Figura 11 – Propriedades com destaque em Dispositivos.

Em seguida informar o endereço para da biblioteca do opensc (em usr/lib/opensc) conforme a figura abaixo:

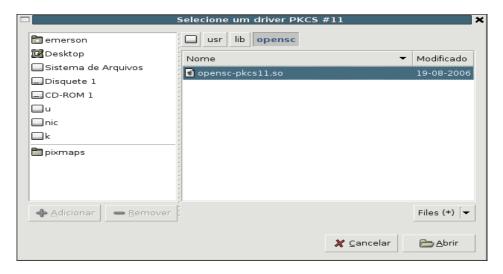


Figura 12 – Selecionando um driver PKCS#11.

Neste momento a ferramenta irá: carregar o dispositivo e ler o certificado armazenado, este tempo deve variar de equipamento para equipamento.

Aguardar até que a tela seja novamente apresentada. Gerenciador de dispositivos de codificação Lista de "Drivers": Clique para ver os certificados Identidades Carregar Fabricante Nome da Bi Arquivo da I OpenSC ... smart ca... /usr/lib/o... Autoridades Descarregar Língua Reiniciar **√**₹ Algoritmos Certificados presentes nos dispositivos conectados: Contatos C=br,O=ICP-Brasil,OU=Caixa Economica Federal,OU O LDAP Diretório Perfil de Clique duas vezes no certificado para ver os detalhes Assinatura Nesta janela você pode ver, adicionar e remover o Aplicar Fechar suporte para dispositivos de codificação.

Figura 13 – Dispositivo e Certificado carregado.

#### 2.2.3.4 Outras configurações.

Conforme a figura 3, existem outras opções configuráveis que são as seguintes:

- Língua: idioma para a interface gráfica.
- Algoritmos: permite selecionar os algoritmos para criptografia e assinatura que a ferramenta suporta.
- Contatos: possibilita configurar quais campos de informação deseja-se para os contatos, os quais podem ser inseridos na ferramenta.
- LDAP: para configurar as informações de acesso a um servidor LDAP (necessitase de auxilio do suporte técnico).
- Diretório: permite definir um diretório padrão de trabalho, esta opção é muito útil,
   principalmente quando faz-se necessário trabalhar com uma grande quantidade de arquivos (marcar a opção preencher lista de arquivos...).
- Perfil de Assinatura: definir o padrão (default) para a assinatura.

#### 2.2.4 Adicionar Contatos.

Esta funcionalidade da ferramenta é especialmente necessária para as tarefas de criptografia, pois permite que o arquivo seja criptografado com a chave pública de um dos contatos cadastrados, o que permitirá o envio seguro deste arquivo.

As funcionalidades são basicamente as mesmas de um leitor de e-mails.

Para acessá-la clique no botão "contatos"



A seguinte tela será apresentada:



Figura 14. Catálogo de Endereços

O botão Configuração tem a mesma funcionalidade do item 2.2.3, os demais são autodescritivos e a funcionalidade "Adicionar" é a mais importante deste item. Ao clicar neste botão a seguinte tela será apresentada.

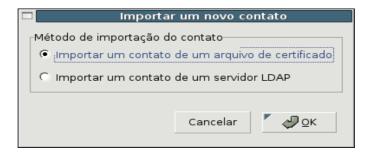


Figura 15. Importar novo contato.

As funcionalidades das duas opções são idênticas, somente que na opção com LDAP é preciso antes configurar o acesso ao servidor (item 2.2.3.4), portanto será exemplificado com um arquivo armazenado localmente: basta clicar no botão OK e informar o diretório onde está o certificado (Chave Pública) que deseja inserir. A tela abaixo será apresentada:

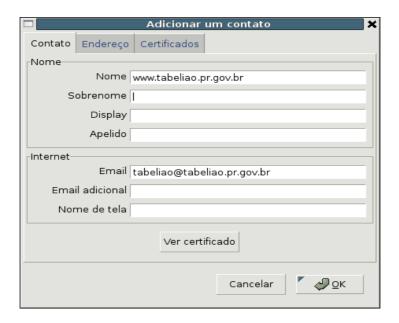


Figura 16. Adicionar Contato

Aqui é possível preencher informações úteis como em uma agenda e ainda na aba Certificados é possível visualizar o certificado digital.

Para criptografar arquivos para uso pessoal é preciso importar o seu próprio certificado, pois assim a ferramenta utilizará a sua chave pública.

#### 2.2.5 Preparação de arquivos.

Com a ferramenta configurada então é possível assinar e/ou criptografar arquivos.

Para estas tarefas é necessário informar à ferramenta quais são os arquivos que serão trabalhados.

A primeira tarefa é localizar os arquivos, caso tenha utilizado a opção "preencher lista de arquivos..." na configuração do diretório padrão (item 2.2.3.4), todos os arquivos neste diretório serão carregados automaticamente quando a ferramenta é iniciada, é útil quando se deseja trabalhar com lotes de arquivos, pois todos os arquivos serão avaliados. Em outros casos é preciso "carregar" o arquivo e para isto deve-se clicar no botão "arquivo" na tela inicial (figura 2).

Em seguida basta encontrar o arquivo ( será aberto o navegador de arquivos) e o mesmo será "carregado" na ferramenta, também é possível selecionar vários arquivos ao mesmo tempo.



Figura 17. Arquivos carregados

Neste ponto a ferramenta possui uma lista de arquivos que poderão ser manipulados.

#### 2.2.6 Codificar/Criptografar arquivos.

Nesta função é possível cifrar (criptografar) arquivos, seja para proteção local ou envio seguro.

Depois do passo anterior (2.2.5) em que carregará o(s) arquivo(s) que deseja cifrar, clicar no botão "codificar"



A tela seguinte é apresentada:

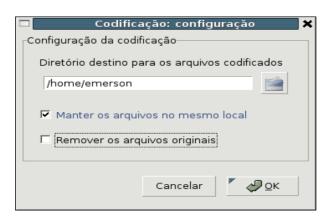


Figura 18. Configurar Codificação

Neste ponto é possível informar um diretório onde serão gerados os arquivos codificados (é necessário Desmarcar a opção "Manter os arquivos no mesmo local"). Também pode ser definido que os arquivos originais serão removidos (maior segurança).

No passo seguinte será pedido para informar o destinatário, que tecnicamente é a chave pública com a qual o arquivo será cifrado e portanto somente o destinatário (dono da chave privada correspondente) é que poderá decifrar o arquivo gerado. No caso de segurança pessoal local é possível utilizar a própria chave pública que também pode ser armazenada nos contatos (item 2.2.4).

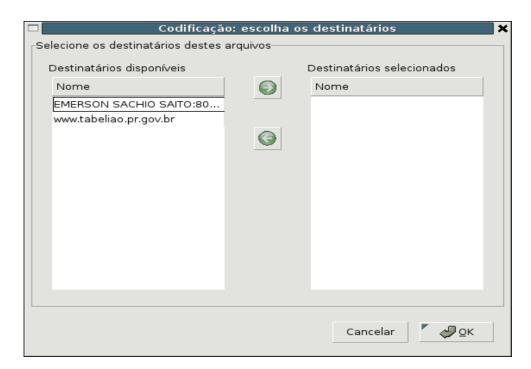


Figura 19. Escolher destinatário.

Assim o arquivo cifrado será gerado.

#### 2.2.7 Decodificar arquivos.

A tarefa de decodificar (decifrar) é inversa à anterior e portanto só é possível para os arquivos criptografados, com a chave pública de uma identidade configurada (item 2.2.3.2), ou ainda utilizando um certificado armazenado em hardware (item 2.2.3.3).

Executar as tarefas do item 2.2.5, agora para o(s) arquivo(s) que deseja decodificar, clicar no botão "decodificar".



Em seguida a figura 15 será apresentada e será possível informar o diretório de destino dos arquivos decifrados e se deseja excluir os arquivos originais cifrados.

Deverá ser informada a senha do certificado para a execução da decifragem conforme as figuras abaixo:



Figura 20 – Informar o PIN (senha pessoal do certificado)

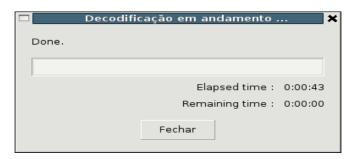


Figura 21 – Decodificação em andamento.

Clique no botão Fechar para finalizar a operação.

Em seguida os arquivos serão gerados no diretório informado, agora sem a criptografia.

#### 2.2.8 Assinatura de arquivos.

Uma outra funcionalidade da ferramenta, e talvez a mais importante, é a geração de assinatura digital.

As tarefas do item 2.2.5 são novamente necessárias para selecionar o(s) arquivo(s) que poderão ser assinados.

Em seguida clique no botão "Assinar"



A tela abaixo será apresentada:

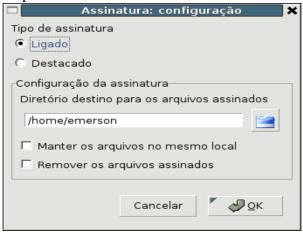


Figura 22. Configuração de Assinatura.

Deve-se informar se a assinatura será do tipo **ligado** o que gera apenas um arquivo com o conteúdo e a assinatura juntos e assim será necessário uma ferramenta como o Criptonit para recuperar os arquivos, ou **destacado** que gerará um arquivo separado para a assinatura e assim uma ferramenta especial só será necessária para validar a assinatura (a segunda forma é a mais recomendada). Da mesma forma que nas funcionalidades anteriores é possível informar o diretório destino e se o arquivo original deve ser excluído (no caso do tipo destacado essa opção não é habilitada) clicando no botão OK a tela seguinte será apresentada:

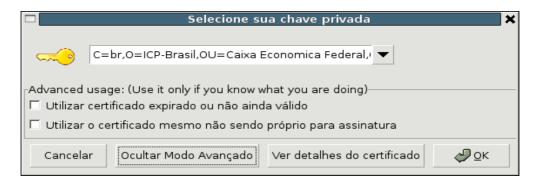


Figura 23. Selecionar Chave privada (certificado)

Caso haja mais de um certificado (identidade em arquivo) configurado, será possível selecionar o desejado, no caso de SmartCard ou Token somente este será apresentado. Ao clicar no botão Mostrar Modo Avançado (na figura foi clicado) serão mostradas algumas opções que podem ser habilitadas caso necessário. Ao clicar no botão OK será necessário informar o PIN (senha do certificado) conforme a figura 20 para geração da assinatura.

A tela abaixo deverá ser apresentada caso o processo esteja correto (clicar no botão Fechar para finalizar o processo):

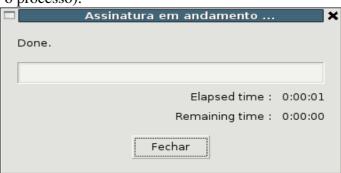


Figura 24 – Assinatura em andamento.

Deve-se lembrar que a assinatura ligada não garante o sigilo das informações, pois o arquivo não estará cifrado.

#### 2.2.9 Verificação de Assinatura.

Esta funcionalidade pode ser considerada "inversa" a anterior, pois pode validá-lo e também pode ser utilizado para verificar quaisquer assinaturas digitais geradas, desde que no padrão reconhecido pela ferramenta, ou como neste caso: no padrão ICP-BRASIL.

As configurações do item 2.2 são necessárias, obviamente, para todos os certificados das assinaturas que se deseja verificar.

De acordo com o passo 2.2.5 localizar e identificar os arquivos assinados para a verificação e em seguida clicar no botão "verificar".



A tela abaixo será apresentada:

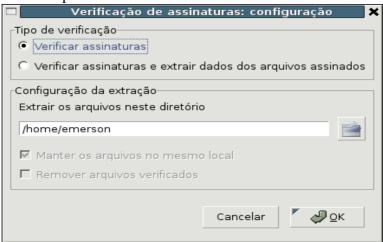


Figura 25. Configuração de verificação de Assinatura.

Neste passo pode-se verificar a assinatura, ou caso o arquivo da assinatura seja do tipo Ligado (um único arquivo), será possível extrair o conteúdo do documento assinado e ainda remover o arquivo de assinatura, neste caso o arquivo original será extraído no local informado.

Ao clicar no botão OK será apresentada a tela seguinte:

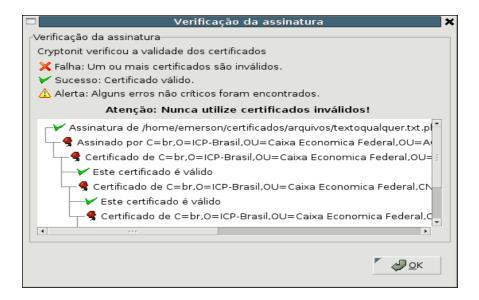


Figura 26. Verificação da Assinatura.

Nesta tela será apresentada toda a cadeia de validação do certificado utilizado para assinatura, sendo sempre a primeira linha a verificação de que a assinatura confere. Atente-se para a legenda:

```
X Falha: Um ou mais certificados são inválidos.
✓ Sucesso: Certificado válido.
∆ Alerta: Alguns erros não críticos foram encontrados.
```

Figura 27. Legenda dos ícones apresentados na validação.

## 3 CONSIDERAÇÕES FINAIS.

Este manual foi redigido utilizando a versão 0.9.7 do Cryptonit e destina-se à orientação do usuário final e não é uma publicação oficial do desenvolvedor.