Aplicativo Assinador

- Guia de Instalação e Operação do Sistema -

Desenvolvido por:

ESEC Tecnologia em Segurança de Dados SCS Q.08 Ed. Venâncio 2000 Bl. B-50 Sl 803 Brasília, DF CEP 70333-900	**Certisign Certificadora Digital S/A** Rua Passeio, 70 - 7 andar, Centro Rio de Janeiro - RJ CEP 20021-290

iti assinador

Índice

1 Apresentação

Este manual objetiva auxiliar o usuário comum na utilização das funcionalidades providas pelo aplicativo Assinador.

2 Instalação

Antes de instalar o aplicativo “Assinador” alguns requisitos devem ser verificados e atendidos. São eles:

- Biblioteca de criptografia “OpenSSL” versão 0.9.7e, ou superior;
- Biblioteca “OpenLDAP” versão 2.0, ou superior;
- Framework “QT” versão 3.3.3, ou superior;
- Biblioteca de acesso a smartcard “OpenSC” versão 0.9.6, ou superior;.

2.1 Instalação via RPM

Uma das formas de distribuição do Assinador é utilizando o formato RPM (“*R*PM *P*ackage *M*anager”). Para instalar o RPM do assinador os seguintes passos deverão ser seguidos

1. Obtenha o arquivo assinador-X.X.X-Y.i5986.rpm onde,
   X.X.X : é a versão do Assinador contida neste RPM;
   Y : é a release do Assinador contida neste RPM;
   OBS: No caso do usuário possuir o CD de instalação, este arquivo poderá ser obtido no diretório “/bin” localizado no diretório raiz do CD.
2. Executar o comando:
   rpm -ivh assinador-X.X.X-Y.i586.rpm

   OBS: o usuário poderá informar o caminho completo do arquivo RPM ou ainda, ir para o diretório que contém o arquivo RPM e simplesmente informar o nome do arquivo.
   O comando acima executará a instalação do software Assinador contido no arquivo RPM indicado.
   Caso haja algum requisito (ou dependências) não atendido, o comando acima mostrará uma mensagem de erro indicando o software que é utilizado pelo Assinador mas que não foi instalado na máquina do usuário.
   Para a distribuição Mandrake há no CD de instalação, no diretório “/bin”, um script chamado “install.sh” o qual irá executar a instalação do RPM do Assinador bem como de qualquer um dos RPMs das dependências do Assinador, caso seja necessário

2.2 Instalação a partir do “tar.gz “

Uma outra forma de instalar o aplicativo Assinador é obter o arquivo “tar.gz” com os fontes do software e compilá-los na máquina do usuário. Para este tipo de instalação os seguintes passos deverão ser seguidos:

1. Obter o arquivo assinador-X.X.X.tar.gz (onde X.X.X é a versão do aplicativo Assinador);
   OBS: No caso do usuário possuir o CD de instalação, este arquivo poderá ser obtido no diretório “/source” localizado no diretório raiz do CD.
2. Descompactar o arquivo “.tar.gz”, executando o comando:
   tar xzvf assinador-X.X.X.tar.gz

   Ao executar este comando um diretório com o nome “assinador-X.X.X) será criado e dentro dele estarão todos os fontes do aplicativo Assinador, e alguns outros arquivos que auxiliarão na compilação destes fontes.
3. Após a descompactação dos fontes, a seguinte sequência de comandos deverá ser executada:
   a) ./configure –prefix=/usr
   b) make

c) make install

Ao final, com sucesso, desta sequência de comandos, o aplicativo Assinador estará instalado é já poderá ser executado.

3 Execução do Assinador

Após a instalação do aplicativo Assinador, o executável “assinador” é armazenado no diretório “/usr/bin”. Para executar o Assinador basta então executar o comando:

/usr/bin/assinador

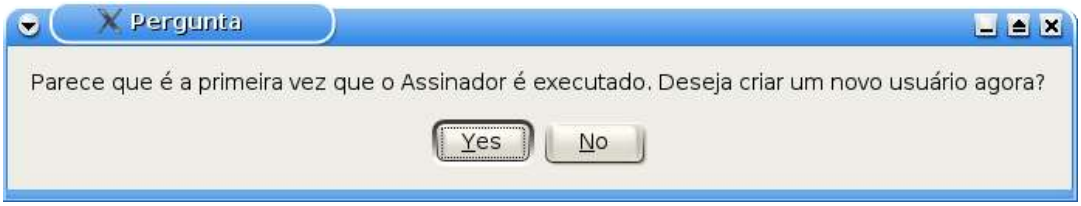
3.1 Primeira execução do Assinador

Durante a primeira execução do aplicativo Assinador, além da visualização da Licença de Software associada ao Assinador, o usuário terá a oportunidade de criar uma “conta de usuário”.

A sequência de tela a seguir ilustra esta circunstância.

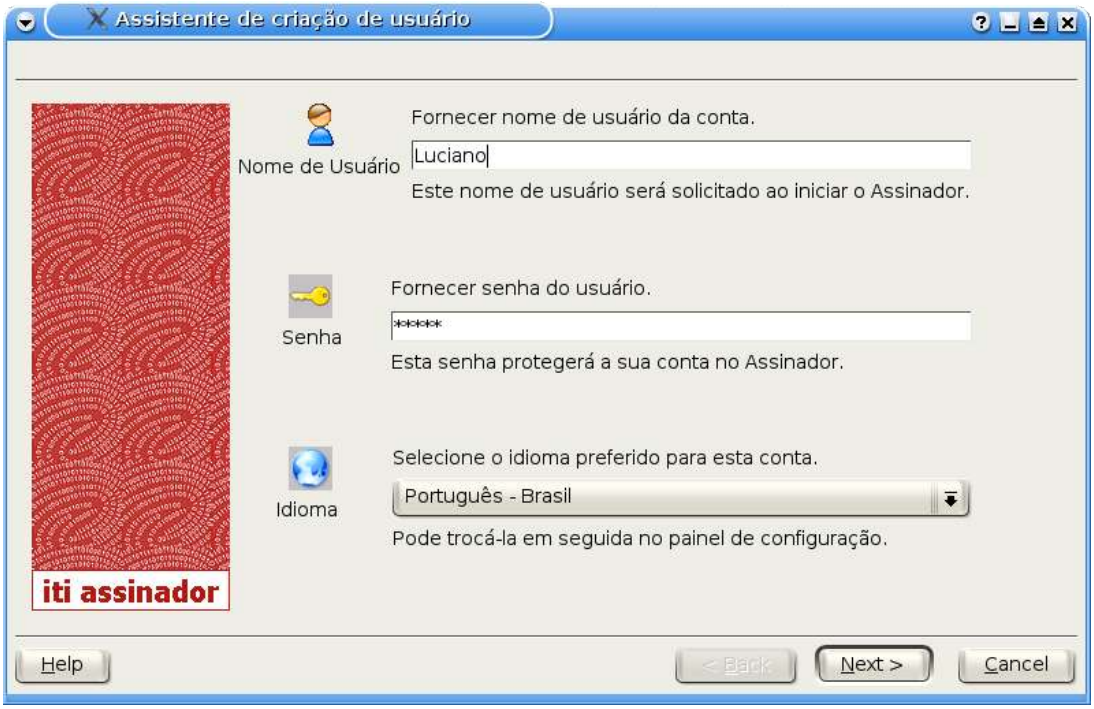
(figura 1 – Licença de software do Assinador)

Na tela acima, o aplicativo apresenta a a licença de software utilizada por ele e solicita ao usuário que este informe se aceita ou não as cláusulas desta licença. Caso usuário defina por recusar esta licença, automaticamente o aplicativo será finalizado. No caso do usuário aceitá-la, uma caixa de diálogo (figura 2) será apresentada ao usuário perguntando se este deseja criar uma nova “conta de usuário”.



(figura 2 – Usuário escolhe por iniciar ou não a criação d euma nova conta de usuário)

É importante que neste momento o usuário responda sim (“yes”) pois somente após a criação de uma “conta de usuário” é que o usuário poderá utilizar o Assinador. Neste caso, o assistente para criação de uma “conta de usuário” será iniciado (figura 3).



(figura 3 – tela inicial do assistente de criação de conta de usuário)

Na tela acima (figura 3), o usuário deverá informar um “nome de usuário” e uma “senha” os quais identificarão este usuário junto ao Assinador.

Nesta versão do Assinador somente o idioma Português do Brasil está disponível.

Após informar o “nome de usuário” e “senha”, o usuário deve clicar no botão “next” para prosseguir com o assistente. Neste momento o assistente mostrará uma tela onde o usuário deverá escolher a forma de obtenção da sua “identidade digital”.

(figura 4 – Escolha do método de importação da chave privada)

O Assinador fornece ao usuário as seguintes opções:

- "Conta em branco": Esta opção informa ao Assinador que o usuário não deseja, neste momento, associar a esta conta nenhuma "Identidade";
- "Importar de um arquivo PKCS#12": indica que a Identidade será obtida a partir de um arquivo PKCS#12. Um arquivo PKCS#12 é normalmente utilizado pelos aplicativos de navegação WEB para transporte de certificados e chave privada protegidos por uma senha.
- "Criar requisição de certificado": indica que o usuário não possui uma Identidade digital e que em função disto deseja criá-la iniciando com a criação de uma requisição de certificado a qual deverá ser encaminhada a uma Autoridade Certificadora para a emissão de um certificado.
- "Importar de um token": indica ao Assinador que o usuário já possui uma Identidade digital e que esta se encontra armazenada em um token criptográfico (Token USB, smart card, etc).

Neste momento, dependendo da escolha que o usuário venha a fazer, diferentes sequências de telas poderão ser apresentadas pelo assistente. Para efeito deste manual, será considerado neste momento a escolha da opção "Importar de um token". As demais opções serão abordadas mais adiante.

ATENÇÃO!!!! Antes de prosseguir com o assistente é necessário que o usuário se certifique que um token (smart card ou token usb)esteja conectado a sua máquina.

Em termos práticos, uma identidade digital é representada por um par certificado, chave privada. Assim sendo, a próxima tela mostrada pelo assistente (figura 5) listará as identidades existentes no token ou seja, mostrará uma lista com o nome do proprietário do certificado cuja chave privada também esteja no token.

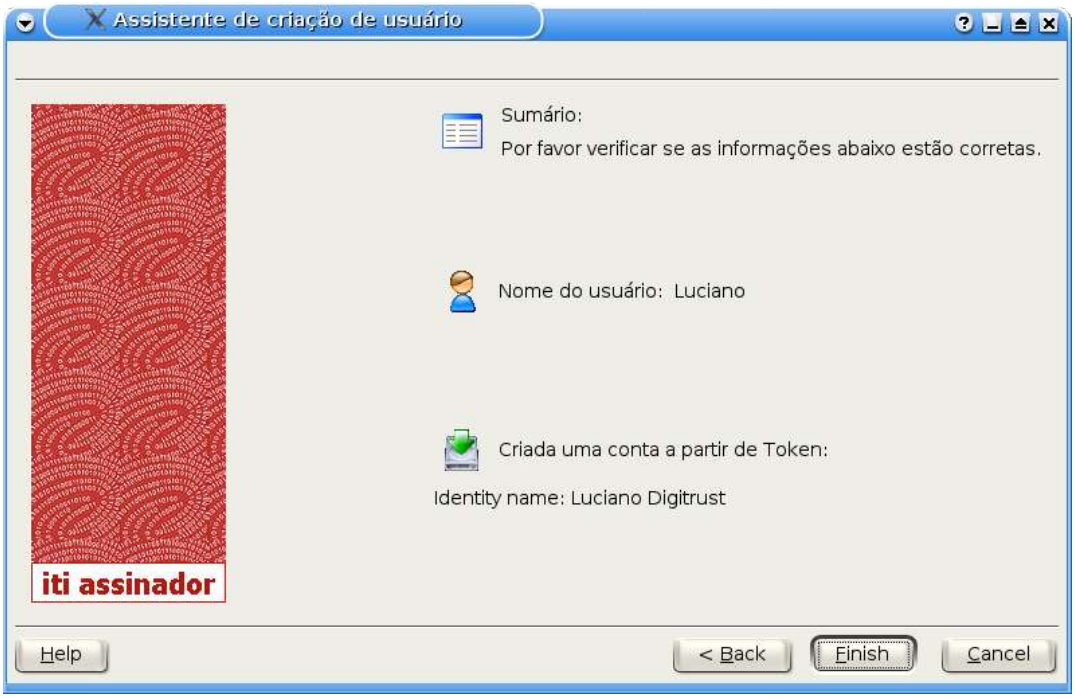
(figura 5 – Importação de identidade armazenada em token)

O usuário deverá então selecionar a chave que ele deseja associar a nova Identidade cujo o nome ele também deve informar nesta tela.

Note que somente após a seleção de uma chave é que os botões “Visualizar certificado” e “OK” são habilitados. O botão “Visualizar certificado” permite a visualização do conteúdo do certificado associado com a chave selecionada pelo usuário. Este botão é util para auxiliar na distinção de duas, ou mais, chaves cujos nomes mostrados na lista sejam o mesmo.

Uma vez que o usuário tenha informado o nome para esta nova Identidade e tenha selecionada a chave desejada, o próximo passo é clicar no botão “OK” para prosseguir com o assistente.

A proxima tela mostrada pelo assistente (figura 6) exibirá o resumo deste processo que fez a criação de uma nova conta de usuário.



(figura 6 – Resumo do assistente de criação de conta de usuário)

Para concluir o assistente clique no botão “Finish”. Neste momento o aplicativo Assinador exibirá a tela de login para que o usuário selecione a conta e forneça a senha associada a ela. Veja como proceder com esta tela no tópico “Próximas execuções.

3.2 Próximas execuções

Em execuções, que não sejam a primeira, o Assinador exibe a tela de login do aplicativo (figura 7). Nesta tela o usuário deverá informar o seu login (o nome da conta de usuário ateriormente criada) e senha para poder utilizar o Assinador. Em seguida deverá clicar no botão para poder efetuar a autenticação dos dados fornecidos.

Se caso o usuário que tenha executado o Assinador ainda não tenha criado nenhuma “conta de usuário”, este poderá fazê-la clicando no botão .

(figura 7 – Tela de login)

Se por algum motivo o usuário desejar interromper a execução do Assinador, basta clicar no botão . 

Após efetuado a autenticação com sucesso o Assinador apresentará a tela principal do aplicativo (figura 8).

(figura 8 – Tela principal do Assinador)

4 Utilização do Assinador

O Assinador fornece basicamente 4 operações:

- Assinar arquivo
- Verificar arquivo assinado
- Encriptar arquivo
- Decriptar arquivo

Independente de suas particularidades, as quais serão abordadas mais adiante, todas as operações acima compartilham um mesmo passo inicial que é a seleção dos arquivos que farão parte da operação.

Para selecionar um ou mais arquivos, o usuário deve inicialmente clicar no botão "Arquivo" ex nte na barra de ferramentas da janela principal. Em seguida o Assinador mostrará uma caixa de diálogo de seleção de arquivo onde o usuário deverá indicar o arquivo desejado. Após a seleção do arquivo a janela principal passará a exibir a lista dos arquivos selecionados (figura 9).

(figura 9 – Lista dos arquivos selecionados)

Note que após a seleção do arquivo os botões associados com as operações “Encriptar”, “Decriptar”, “Assinar” e “Verificar” foram habilitados.

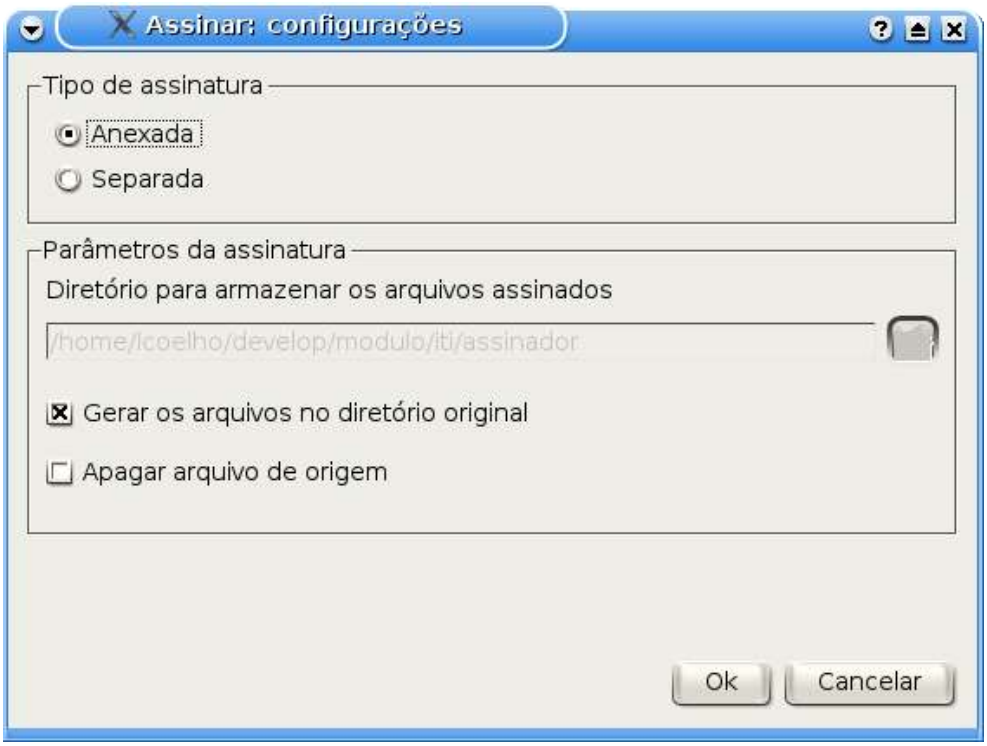
DICA!!! Para a remoção de um arquivo da lista, basta selecioná-lo e em seguida pressionar a tecla “Delete”.

Vejamos agora como executar cada uma das operações.

4.1 Assinatura de arquivos

Para proceder com a assinatura de um arquivo o usuário deverá, após a seleção do arquivo conforme visto anteriormente, clicar no botão “Assinar” existente na barra de ferramentas do Assinador.

Neste momento o Assinador exibirá uma tela (figura 10) onde o usuário poderá configurar como a assinatura deverá ser efetuada.



(figura 10 – Configurar assinatura)

Na tela de configurações da assinatura as seguintes opções estarão disponíveis:

- "Tipo de assinatura"
  - "Anexada": Neste tipo de assinatura é criado um arquivo PKCS#7 contendo a assinatura e o arquivo assinado. Nesta caso o arquivo contendo a assinatura ficará independente do arquivo original ou seja, o arquivo original poderá ser apagado mas ainda assim a assinatura poderá ser verificada.
  - "Separada": Neste tipo um arquivo PKCS#7 é criado contendo somente a assinatura. Nesta opção o arquivo que foi assinado deverá estar no mesmo diretório do arquivo de assinatura quando este for verificado.
- "Gerar os arquivos no diretório original": se selecionada esta opção informa ao Assinador que o arquivo PKCS#7 deverá ser criado no mesmo local onde se encontra o arquivo sendo assinado. Por exemplo, se o usuário deseja assinar o arquivo "/tmp/teste_file.txt" então o arquivo PKCS#7 será criado no diretório "/tmp". Caso esta opção não esteja selecionada, o usuário poderá então informar no campo "Diretório para armazenar os arquivos assinados" o diretório desejado.
- "Apagar arquivo de origem": o usuário informar ao assinador que após a assinatura o arquivo que foi assinado deverá ser apagado. Note que o sistema não permite que esta opção seja selecionada ao mesmo tempo que o tipo de assinatura "separada" esteja selecionada.

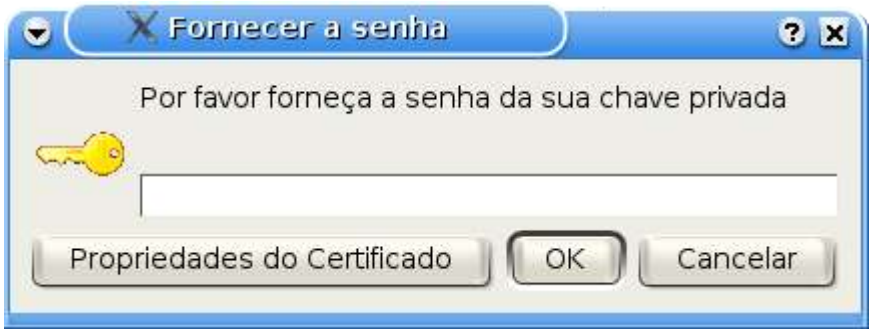
Concluída a configuração da operação de assinatura o usuário deve clicar no botão "Ok" para prosseguir com o processo de assinatura.

Como o usuário pode possuir várias Identidades, i.e. várias chaves privadas cadastradas, a próxima tela apresentada (figura 11) pelo Assinador permitirá ao usuário a seleção de qual Identidade este deseja usar para assinar o arquivo.

(figura 11 – Selecão da Identidade que assinará)

DICA!!! Caso a lista de Identidades possua duas ou mais Identidades com o mesmo nome, use o botão "Detalhes do Certificado" para visualizar o conteúdo do certificado associado à Identidade selecionada e com isso decidir qual identidade usar.

Após selecionar a Identidade o usuário deverá clicar no botão "Ok". Neste momento o Assinador apresentará uma caixa de diálogo solicitando a senha de acesso a chave privada desta Identidade (figura 12).



(figura 12 – Solicitação da senha de acesso à chave privada)

Após fornecer a sua senha o usuário deverá clicar em "Ok" indicando desta forma ao Assinador que este pode efetivamente dar início ao processo de assinatura do arquivo. Neste momento a tela poderá ficar "congelada" por alguns instantes.

Concluída a assinatura do arquivo o Assinador automaticamente removerá da lista de arquivos a entrada associada ao arquivo assinado.

O Assinador permite ainda uma processo especial de assinatura denominado "co-assinatura". Neste processo o Assinador adiciona a um arquivo de assinatura uma nova assinatura. Este processo é transparente para o usuário. Para ser executado basta que o usuário adicione a lista de arquivos um arquivo de assinatura (um arquivo PKCS#7)

4.2 Verificação de assinatura

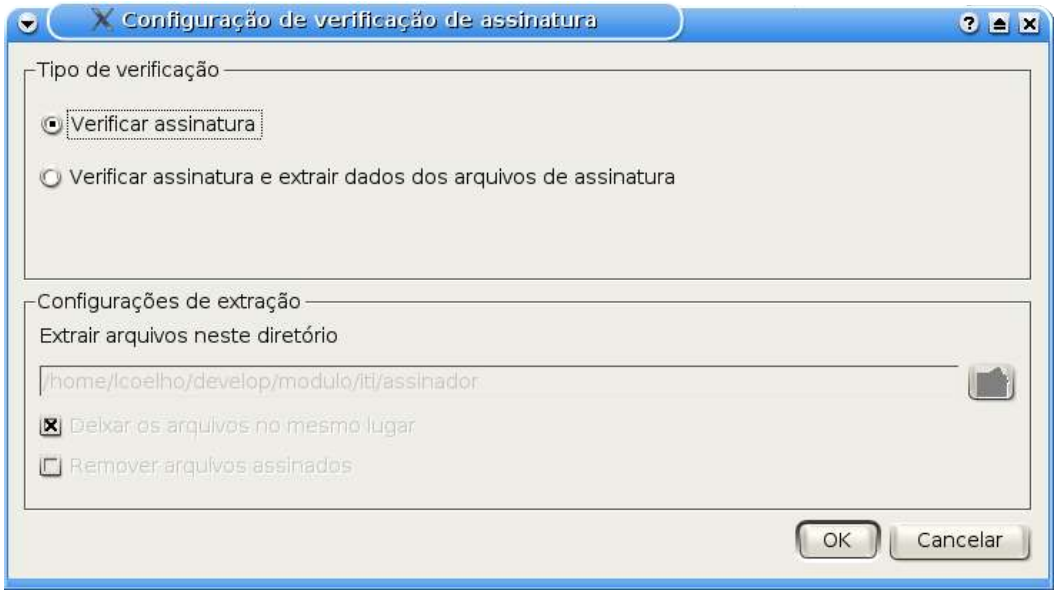
Para verificar uma assinatura o usuário deverá primeiramente selecionar o arquivo PKCS#7 associado à assinatura desejada, conforme já explicado.

Como visto anteriormente, o tipo de assinatura efetuada afetará diretamente na forma como o Assinador fará a Verificação da mesma. Se a assinatura gerada foi do tipo "Separada" então o arquivo assinado deve estar no mesmo diretório do arquivo PKCS#7 sendo verificado, caso contrário a assinatura não poderá ser verificada. Já a assinatura do tipo "Anexada" não possui esta limitação visto que o arquivo que foi assinado também está presente no arquivo PKCS#7 que contém a assinatura.

Para auxiliar nesta distinção de tipos o Assinador apresenta na lista de arquivos a informação do tipo de arquivo. Este tipo será “Signed file” no caso de assinatura “Anexada” e “Dettached signature” no caso de assinatura “Separada”. Veja o exemplo a seguir.

Selecionados os arquivos, o usuário deverá clicar no botão “Verificar” para então dar início erificação dos arquivos.

Neste momento o Assinador exibe para o usuário a tela de configurações da Verificação (figura 14).



(figura 14 – Configurações da Verificação)

Nesta tela o usuário se deparará com as seguintes opções:

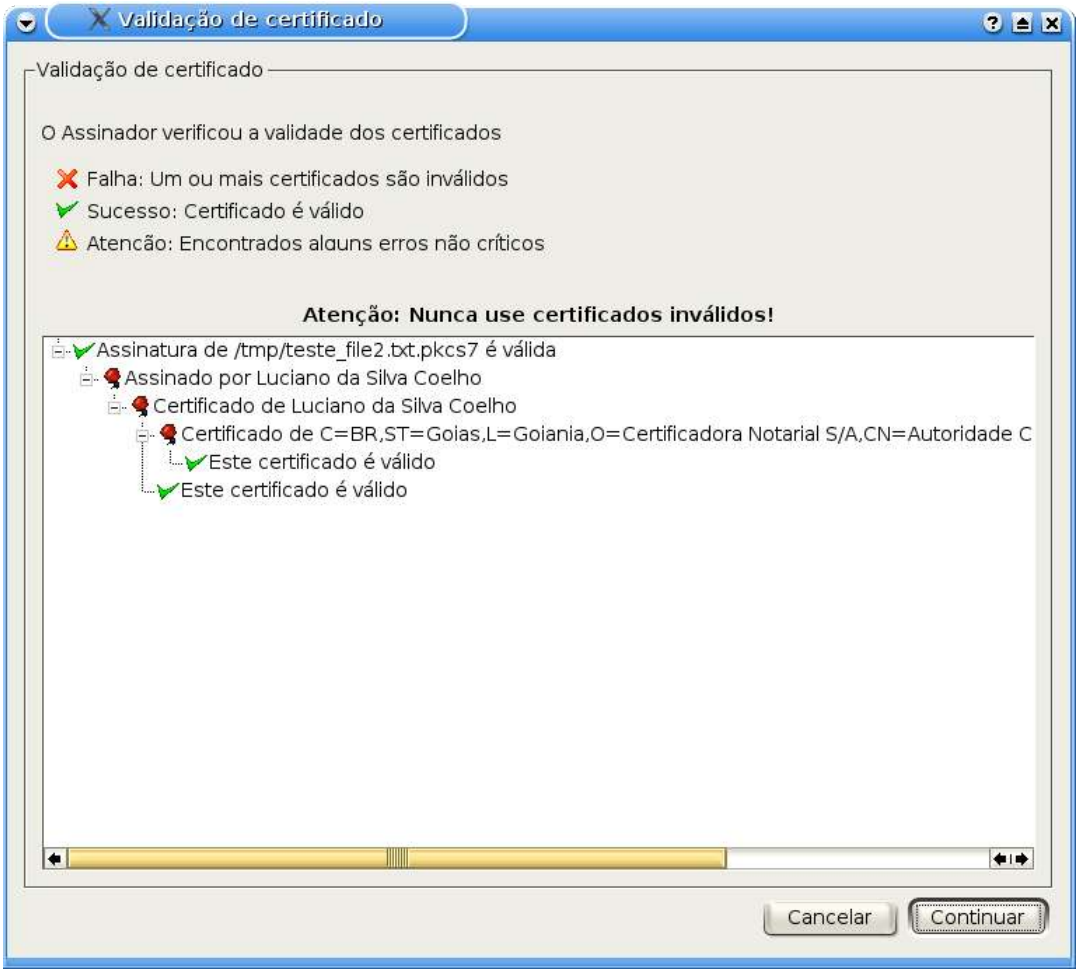
- “Tipo de Verificação”
  - “Verificar assinatura”: O assinador simplesmente verifica a assinatura.
  - “Verificar assinatura e extrair dados dos arquivos de assinatura”: O Assinador além de verificar a assinatura e ele remove do arquivo de assinatura o arquivo original. Esta opção somente é válida no caso de arquivos de assinatura do tipo “Anexada”.
- “Deixar os arquivos no mesmo lugar”: se selecionada esta opção informa ao Assinador que o arquivo assinado obtido do arquivo de assinatura deverá ser armazenado no

mesmo local onde se encontra o arquivo de assinatura. Por exemplo, se o usuário deseja verificar o arquivo "/tmp/teste_file.txt.pkcs7" então o arquivo contido nele será armazenado no diretório "/tmp". Caso esta opção não esteja selecionada, o usuário poderá então informar no campo "Extrair arquivos neste diretório" o diretório desejado.

- "Remover arquivos assinados": Informa ao assinador que o arquivo de assinatura do tipo "Anexada" deve ser apagado após a sua verificação.

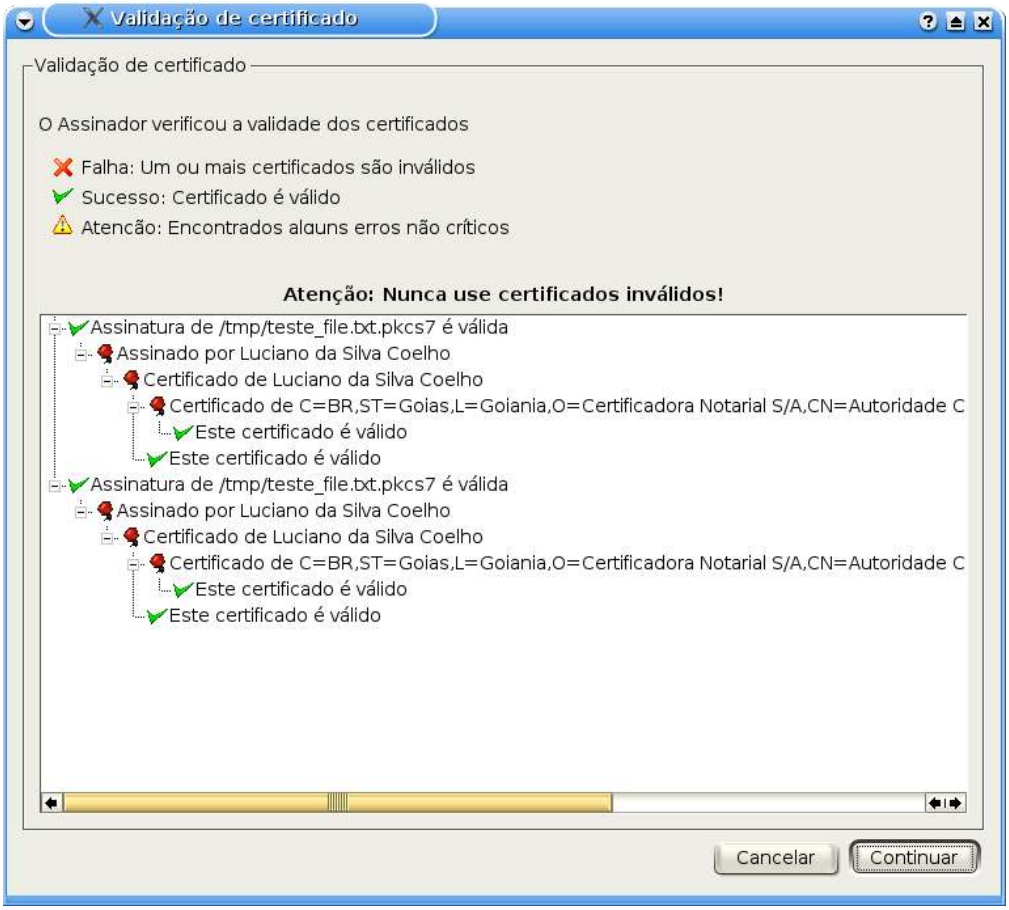
Concluída as configurações da operação de Verificação, o usuário deve clicar no botão "Ok" para prosseguir com o processo de verificação.

O Assinador mostrará uma tela com o resultado da Verificação (figura 15).



(figura 15 – Resultados da Verificação).

No caso de um arquivo de assinatura que contenha mais de uma assinatura, uma co-assinatura, o resultado da verificação mostrará o resultado de todas as assinaturas existentes (figura 16).

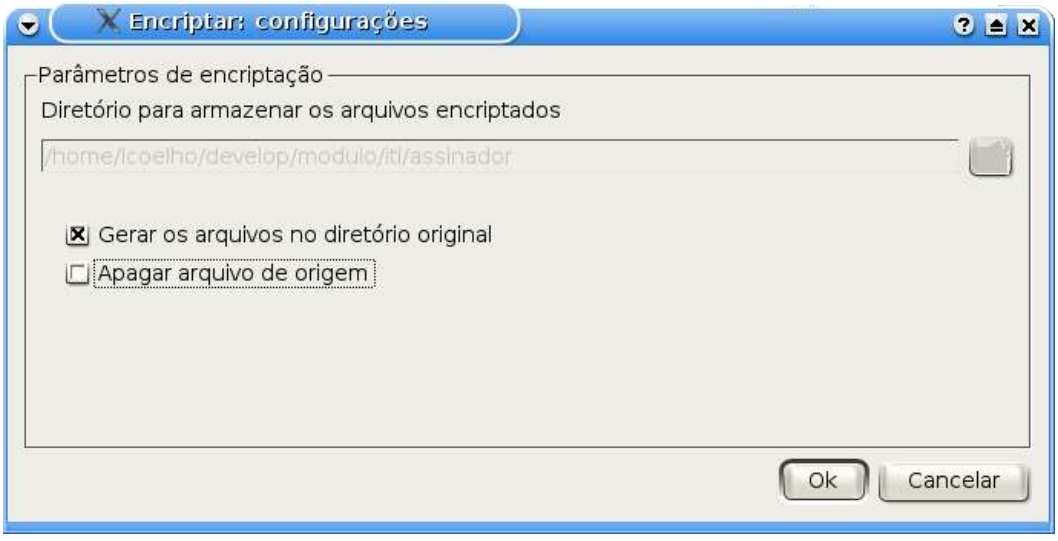


(figura 16 – Resultado da verificação de uma arquivo que foi co-assinado).

4.3 Encriptação de arquivos

Para encriptar um arquivo o usuário precisa inicialmente selecionar o arquivo desejado, conforme já explicado, e em seguida clicar no botão “Encriptar” existente na barra de ferramentas da janela principal do Assinador.

Neste momento o Assinador exibirá uma tela onde o usuário poderá definir algumas configurações para o processo de encriptação (figura 17).

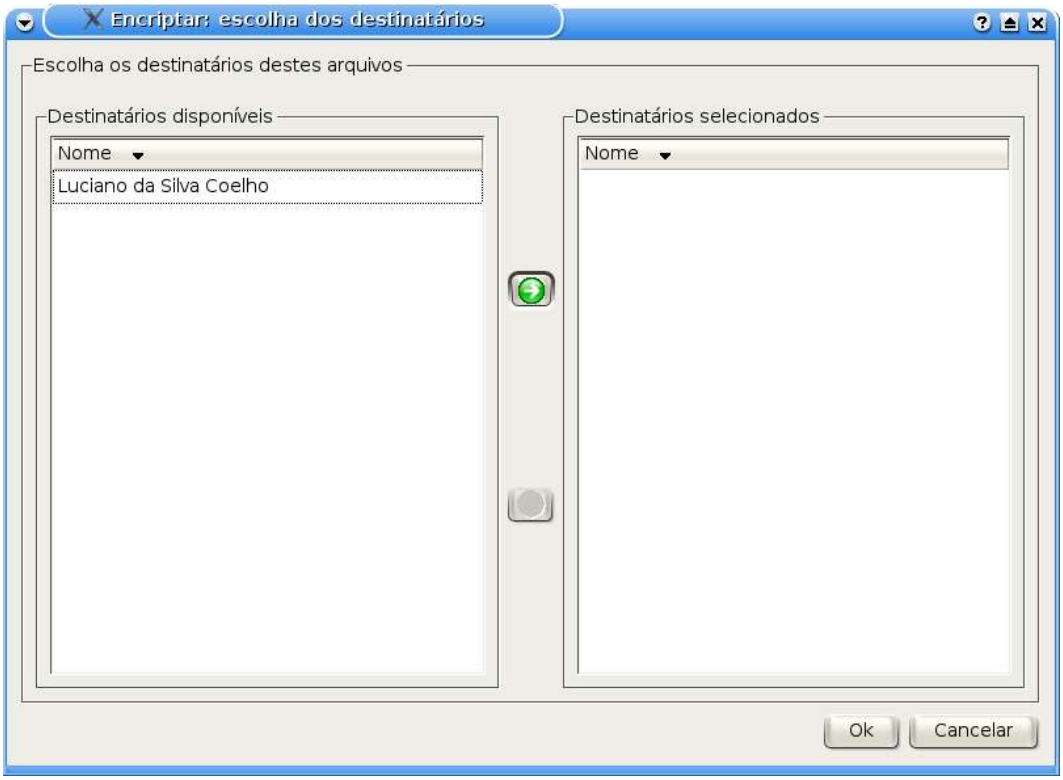


(figura 17 – Configurações para a Encriptação)

Nesta tela de configuração o usuário encontrará as seguintes opções:

- "Gerar os arquivos no diretório original": Se definida esta opção informa ao Assinador que o usuário deseja que o arquivo resultante da encriptação seja armazenado no mesmo local onde se encontra o arquivo original. Caso esta opção não esteja definida, o campo "Diretório para armazenar os arquivos encriptados" será habilitado e nele o usuário poderá indicar o diretório desejado.
- "Apagar arquivo de origem": Indica ao Assinador que o arquivo original deverá ser apagado após a geração do arquivo encriptado.

Para dar prosseguimento à operação de encriptação, o usuário deve clicar no botão "Ok". Em seguida o Assinador exibirá a tela (figura 18) para seleção dos Contatos para os quais o arquivo deverá ser encriptado.

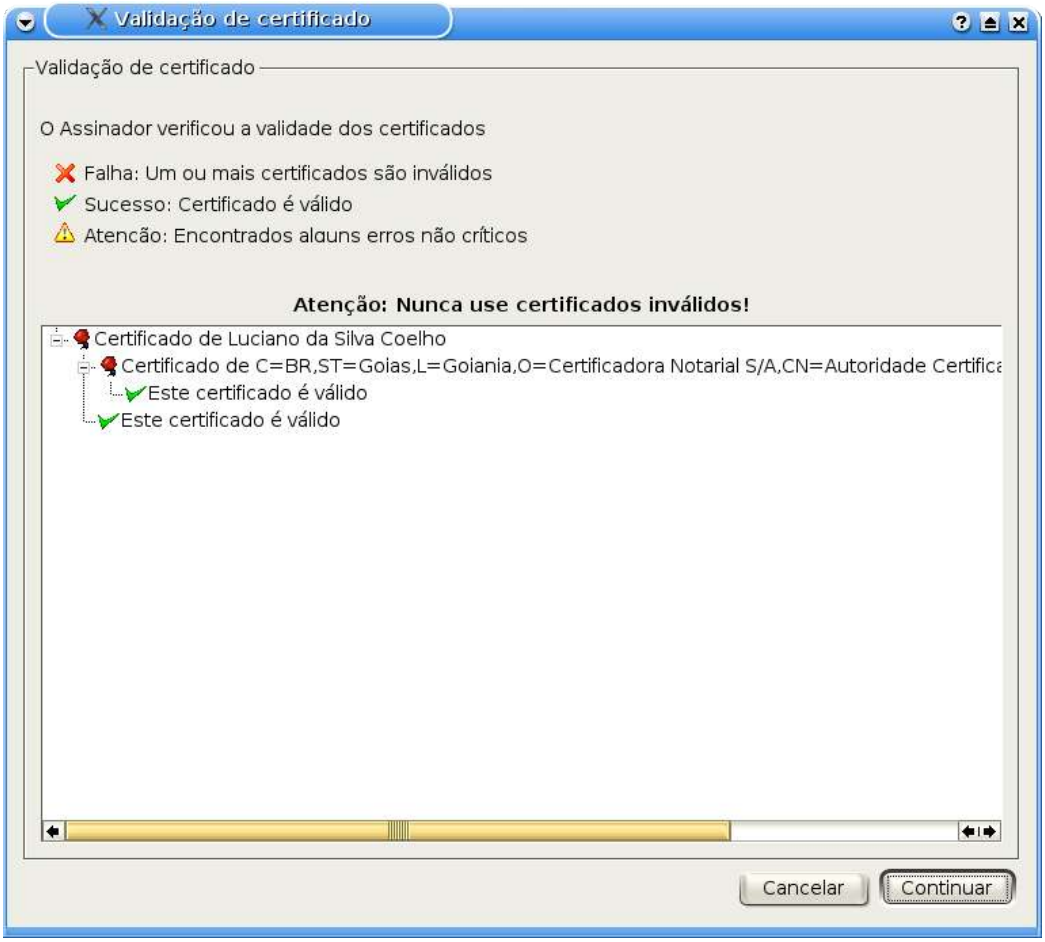


(figura 18 – Seleção dos Contatos que serão destinatários do arquivo encriptado)

Nesta tela o usuário deverá selecionar da lista de "Distinatários disponíveis" aqueles que serão os "Destinatários selecionados" para receber o arquivo encriptado. Este processo poderá ser feito selecionando na lista de "Destinatários disponíveis" um Contato e em seguida clicando no botão o que fará com que o Contato seja transportado para a lista "Destinatários selecionados". O mesmo resultado porde ser obtido dando um clique duplo em um Contato existente na lista "Destinatários disponíveis".

Caso um Contato tenha sido transportado por engano para a lista "Destinatários selecionados", ele poderá ser removido usando o tão ou então dando um clique duplo sobre ele.

Após selecionar todos os contados desejados, o usuário deve clicar no botão "Ok" para prosseguir com o processo de encriptação. O Assinador exibe então uma tela (figura 19) com o resultado da verificação dos certificados de todos os Contatos selecionados.



(figura 19 – Validação dos certificados dos Contatos)

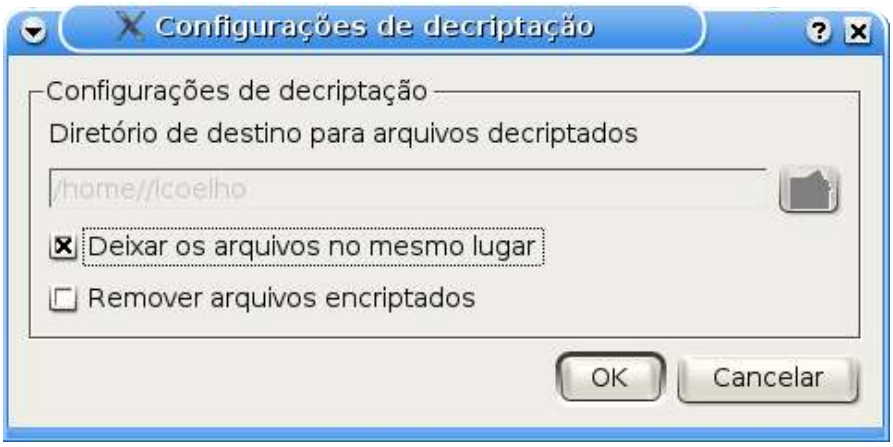
Para efetivamente encriptar o arquivo o usuário deve então clicar no botão "continuar".

Automaticamente o Assinador remove da lista de arquivos a entrada relacionada ao arquivo que foi encriptado.

4.4 Decriptação de arquivo

Para decriptar um arquivo o usuário precisa, primeiramente, selecionar o arquivo desejado. Em seguida, o usuário deve clicar no botão "D riptar" existente na barra de ferramentas da janela principal do Assinador.

O Assinador por sua vez exibirá a tela para configuração da operação de decriptação (figura 20).

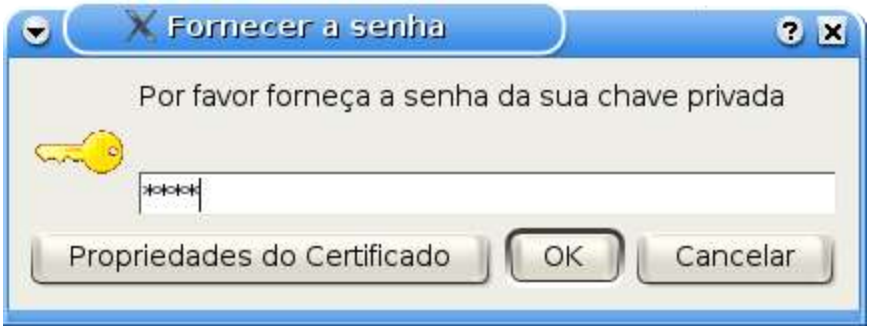


(figura 20 – Configurações da Decriptação)

Nesta tela o usuário poderá alterar as seguintes opções:

- "Deixar os arquivos no mesmo lugar": Se esta opção estiver definida o Assinador gravará no mesmo lugar onde se encontra o PKCS#7 encriptado, o arquivo decriptado. Caso esta opção não seja definida, o campo "Diretório de destino para arquivos decriptados" será habilitado e nele o usuário poderá informar o diretório desejado.
- "Remover arquivos encriptados": Esta opção quando selecionada faz com que o Assinador apague o arquivo PKCS#7 encriptado após este ser decriptado.

Concluída a configuração o usuário deve clicar no botão "Ok" para que o processo de decriptação seja continuado. Em seguida o Assinador apresenta uma tela (figura 21) solicitando ao usuário que este informe a senha de acesso a chave privada que propociará a decriptação do arquivo.



(figura 21 – Solicitação da senha de acesso a chave privada)

Nesta tela o usuário tem a opção de visualizar as informações do certificado associado à chave utilizada na decriptação do arquivo. Esta opção é obtida clicando no botão "Propriedades do Certificado". Para efetivar o processo de decriptação o usuário necessita clicar no botão "Ok". Durante o processo de decriptação do arquivo a interface gráfica poderá aparecer "congelada" retornando ao normal com a conclusão da operação.

5 Gerenciamento de Contatos

Como visto no início deste manual, um Contato faz a ligação entre informações de um indivíduo e o seu certificado (chave pública). Pelo Assinador o usuário poderá gerenciar todos os Contatos para os quais o usuário poderá enviar algum arquivo encriptado.

Para ter acesso as funcionalidades de gerência dos Contatos, o usuário deve clicar no botão "Contato" existente na barra de ferramentas da janela principal do Assinador. Em resposta a esta ação o Assinador exibirá a tela a seguir:

(figura 22 – Gerenciamento de Contatos)

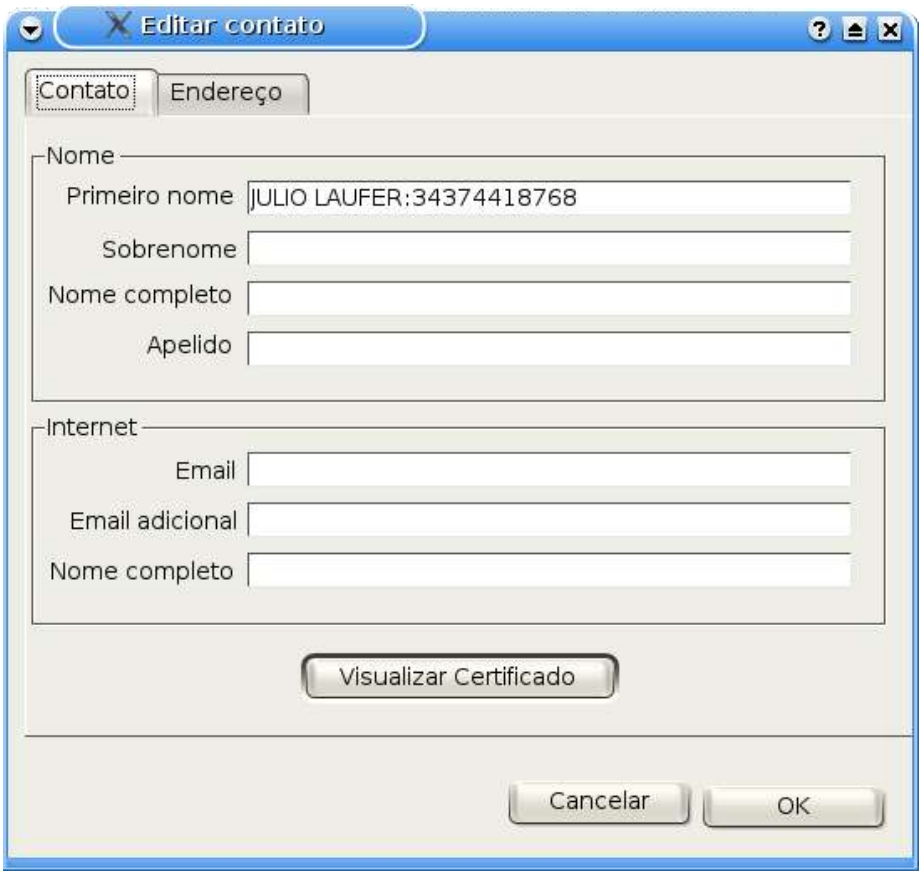
Na tela acima o usuário poderá executar as seguintes ações:

- "Adicionar": Adiciona um novo contato a lista.
- "Remover": Remove da lista de Contatos o Contato selecionado.
- "Fechar": Fecha a tela de Gerenciamento de Contatos

5.1 Adição de novo Contato

Para adicionar um novo Contato o usuário deverá clicar no botão "Adicionar" existente na barra de ferramentas da tela de Gerenciamento de Contatos. O Assinador por sua vez exibirá uma caixa de seleção de arquivo que através da qual o usuário deverá informar o arquivo contendo o certificado do novo Contato. O certificado poderá estar codificado em DER ou PEM.

Uma vez selecionado o arquivo contendo o certificado do Contato o Assinador apresentará uma tela onde o usuário poderá fornecer algumas informações adicionais sobre o Contato. Note que alguns campos já são apresentados preenchidos com informações obtidas do certificado carregado. O usuário tem ainda a oportunidade de verificar as informações do certificado do Contato antes de efetivar a criação do novo Contato. Para tanto, o usuário deve clicar no botão "Visualizar Certificado".



(figura 23 – Edição de um novo Contato)

Fornecidas todas as informações possíveis, o usuário deve clicar no botão “Ok” para continuar com a criação do Contato.

Dependendo do certificado associado ao novo Contato, o Assinador poderá apresentar uma caixa de diálogo (figura 24) perguntando ao usuário se ele deseja carregar a CRL associada ao certificado deste novo Contato. Mesmo não sendo obrigatório, é uma boa prática permitir ao Assinador que ele faça a recuperação desta CRL.

(figura 24 – Permissão para recuperar CRL para o certificado do novo Contato).

ATENÇÃO!!! Para que uma CRL seja recuperada e carregada com sucesso para dentro do Assinador, é necessário que exista uma cadeia de certificados que valide o certificado do novo Contato, previamente carregada no Assinador.

5.2 Remoção de um Contato

Para remover um Contato o usuário basta selecioná-lo na lista de contatos apresentada pela tela de Gerenciamento de Contatos, e em seguida clicar no botão “Remover” .

6 Configurações do Assinador

Neste tópico serão abordados algumas outras configurações existentes no Assinador e acessíveis pela opção “Configurações”
contida na barra de ferramentas da janela principal do Assinador.

Como se pode observar na tela abaixo (figura 25) o Assinador fornece as seguintes configurações:

- Identidades: Permite a gerência das Identidades cadastradas para este usuário. Cada Identidade pode ser encarada como uma chave privada que este usuário tem accesso.
- Autoridades: Gerencia a lista de Autoridades Certificadoras cadastradas no Assinador por este usuário;
- Idioma: Esta opção permitiria a alteração do Idioma utilizado pelo Assinador. Na versão atual somente o Idioma Português do Brasil está disponível.
- Algoritmos: Permite a configuração de alguns algoritmos criptográficos utilizados pelo Assinador.

Vejamos a seguir detalhes sobre cada uma destas opções.

(figura 25 – Configurações do Assinador)

6.1 Gerenciamento das Identidades

O Assinador requer que ao menos uma Identidade seja cadastrada para que algumas das suas funcionalidades sejam desempenhadas com sucesso.

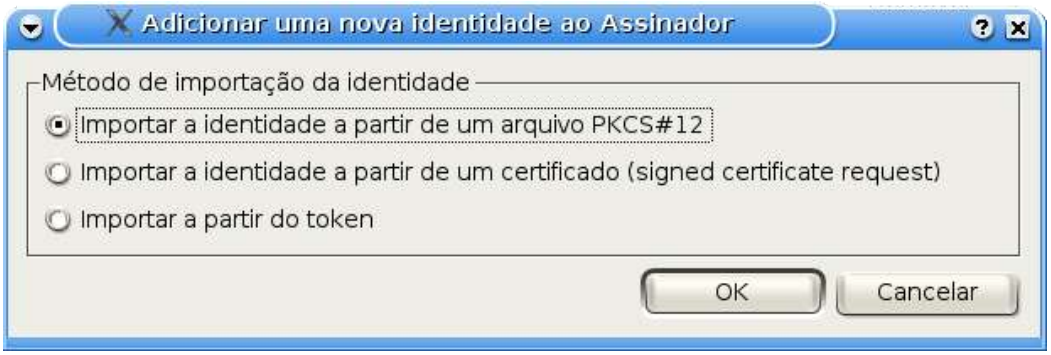
Uma Identidade é, em termos práticos, a indicação de uma chave privada que o usuário tem acesso e que com ela pode executar ações como assinar e decriptar dados enviado em sigilo para ele. Como somente a chave privada pode ser insuficiente para precisar quais operações ela é tem permissão para executar, um certificado digital, par da chave privada, é também necessário.

Para gerenciar as sua Identidades o usuário deve clicar no botão “Identidades” localizado na parte esquerda da tela de Configurações.

Selecionada a opção “Identidades” o conteúdo da porção centro-direita da tela de Configurações é alterado e passa a exibir a lista de Identidades cadastradas e um conjunto de botões que representam as operações de gerenciamento destas Identidades.

6.1.1 Adicionar Identidade

Para adicionar uma nova Identidade o usuário deve clicar no botão “Adicionar”. Em seguida o Assinador exibira uma caixa de diálogo solicitando ao usuário o método de importação a ser utilizado.



(figura 26 – Seleção do método de importação da chave privada)

As opções disponíveis são:

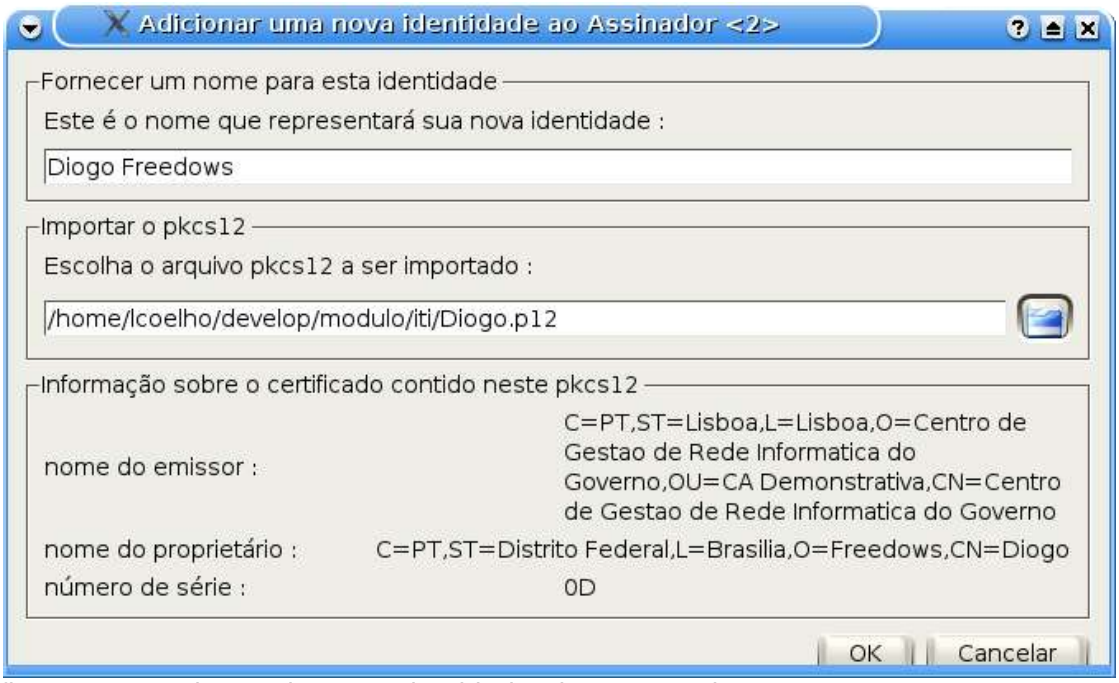
- “Importa a identidade a partir de um arquivo PKCS#12”: esta opção permite a importação da chave privada e certificado armazenados em um arquivo PKCS#12.
- “Importar a identidade a partir de um certificado (signed certificate request): nesta opção será realizada a importação de um certificado o qual é a resposta a uma solicitação de certificado feita previamente.
- “Importar a partir do token”: permite a utilização de uma chave privada armazenada em um token criptográfico (Token USB, smart card, etc) e a importação do certificado armazenado nele.

Como a opção “Importar a partir do token” já foi abordada no tópico “Primeira execução do Assinador”, então somente as demais opções serão exploradas daqui em diante.'

Importar a partir de um PKCS#12

Um arquivo PKCS#12 é um arquivo cuja estrutura permite o transporte seguro de certificados e chaves privadas entre máquinas. Normalmente, tais informações são armazenadas no arquivo PKCS#12 protegidas por uma senha.

Uma vez tal opção tenha sido escolhida pelo usuário o Assinador exibirá a seguinte tela onde o usuário poderá indicar o nome do arquivo PKCS#12 e um nome para esta Identidade.



(figura 27 – Cadastro de nova Identidade via PKCS#12)

Para efetivar a carga da nova Identidade o usuário precisa clicar em “Ok”.

Importar a partir de um certificado

Nesta opção o usuário desejará importar somente um certificado o qual foi gerado a partir de uma requisição de certificado construída pelo usuário ou seja, o usuário já possui no Assinador a chave privada, só está faltando o certificado o qual indicará quais ações poderão ser executadas usando a chave privada associada a ele.

Uma vez tal opção tenha sido escolhida pelo usuário o Assinador exibirá uma caixa de seleção de arquivo de forma que o usuário possa informar o arquivo contendo o certificado a ser carregado.

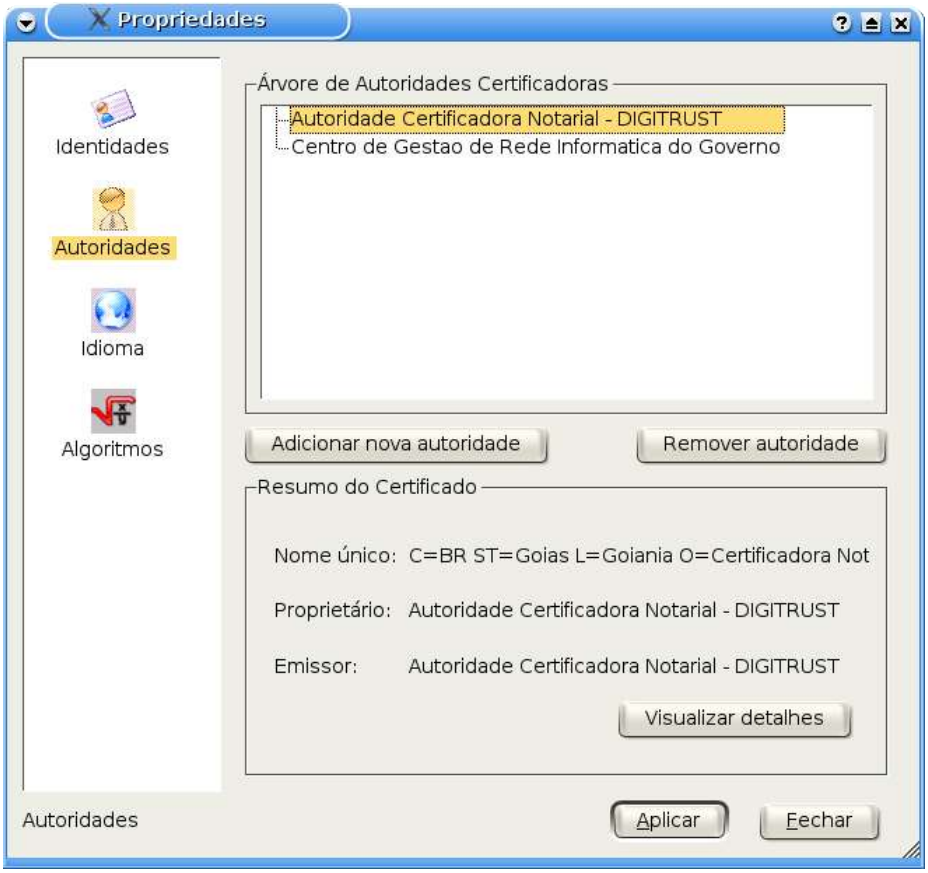
6.1.2

6.2 Gerenciamento de Autoridades Certificadoras

Dentre as tarefas executadas pelo Assinador durante as operações de assinatura, verificação, encriptação e decriptação, podemos destacar aqui a tarefa a validação de certificado baseado na verificação da sua cadeia de certificados. Uma cadeia de certificados é uma sequência de certificados onde um certificado assina o anterior. Desta forma, confiando em um único certificado, digamos a Autoridade Certificadora raiz de uma hierarquia como a da ICP-Brasil, podemos checar a veracidade de um conjunto de outros certificados.

O Assinador ao ser instalado não possui nenhuma Autoridade Certificadora previamente cadastrada. A medida que novas Identidades são adicionadas um conjunto de Autoridades Certificadoras também são automaticamente adicionadas. Além deste comportameto automatizado, o usuário pode ainda manualmente cadastrar, ou remover, outras Autoridades. Para ter acesso a estas funcionalidades o usuário necessita selecionar a opção “Autoridades” existente na tela de Configurações do Assinador.

Após selecionada esta opção o Assinador exibe a seguinte tela:



(figura 28 – Gerenciamento de Autoridades)

Nesta tela as seguinte opções estão disponíveis para o usuário:

- "Adicionar nova autoridade": Permite ao usuário a carga de um novo certificado de Autoridade Certificadora a partir de um arquivo.
- "Remover Autoridade": Permite a remoção de uma Autoridade Certificadora previamente selecionada.
- "Visualizar detalhes": Permite a visualização do conteúdo do certificado da Autoridade selecionada na lista disponível.

6.3 Configuração dos Algoritmos

O modo de configuração do Assinador permite que o usuário defina quais algoritmos criptográficos deseja utilizar nas operações de assinatura e encriptação.

Pelo fato de o Assinador ter a definição do algoritmo assimétrico fixado como sendo o RSA, somente os algoritmos simétricos – usados na encriptação - , e o algoritmo de hash – usado na assinatura – podem ser personalizados pelo usuário.

Dependendo da versão da biblioteca OpenSSL instalada na máquina do usuário, o Assinador permitirá a escolhe dos seguintes algorítmos simétricos: RC2, RC4, RC5, Blowfish, CAST, IDEA e AES. Também dependente da versão da biblioteca OpenSSL instalada, a lista de funções de hash disponível é: MD2, MD4, MD5, SHA1, MDC2,
ripemd e rmd160.

7 Informações sobre o software

O aplicativo Assinador foi desenvolvido pela e-Sec Tecnologia em Segurança de Dados em parceria com a Certisign Certificadora Digital a partir dos códigos fonte do aplicativo Cryptonit desenvolvido pela IDEALX (www.idealx.org).

Este software utiliza os seguintes outros softwares livres:

- QT
- OpenSSL
- OpenLDAP
- OpenSC
- PCSC-lite
- Um conjunto de drivers PCSC-lite para leitoras e tokens USB.