PLATAFORMA DE DESENVOLVIMENTO PINHÃO PARANÁ

MANUAL DE ATENDIMENTO AO USUÁRIO DE CERTIFICADO DIGITAL

Março – 2007

Sumário de Informações do Documento

Tipo do Documento: Manual

Título do Documento: INSTALAÇÃO DE CERTIFICADO DIGITAL EM APLICAÇÃO WEB-JBOSS.

Estado do Documento: EB (Elaboração)

Responsáveis: Emerson Sachio Saito

Palavras-Chaves: Certificado, Digital, Certificação, Aplicação, WEB, ICP-BRASIL, Tabelião.

Resumo: Este é um guia para equipes de atendimento e suporte de aplicativos que utilizem Certificados Digitais padrão ICP-BRASIL, este material faz parte do proto-agente Tabelião que é parte integrante da plataforma de desenvolvimento PINHÃO-PARANÁ.

Número de páginas: 16

Software utilizados: OpenOffice Writer

Versão	Data	Mudanças
1.0	10/03/2007	Criação (Revisão: Cíntia A Evangelista)
1.1	15/05/2007	Atualização da lista de perguntas freqüentes - inclusão.

SUMÁRIO

1 CONTEXTO GERAL

1.1 Introdução

A CELEPAR através da GIC (Gerência de Inovação Corporativa) definiu algumas normas para utilização de Certificados Digitais, sendo que a principal delas é que será adotado o padrão ICP-BRASIL para quase todos os níveis de certificação, excetuando-se apenas àquelas aplicações de uso estritamente interno e estes casos devem ser resolvidos por consulta a área demandante. Portanto é necessária a aquisição de um Certificado Digital de uma Autoridade de Registro, vinculada a uma Autoridade Certificadora CREDENCIADA junto à ICP-BRASIL, para utilização deste manual.

Outros aspectos e normas relacionados à Certificação Digital são abordados no curso de Nivelamento Teórico, que é oferecido pela GIC através do projeto TABELIÃO do qual este documento faz parte. Sendo assim, é importante para quem utilizar este manual participar do referido curso.

O TABELIÃO é um proto-agente integrante da plataforma de desenvolvimento PINHÃO-PARANÁ e é o componente responsável pelas tarefas de certificação digital nos sistemas que o utilizam.

1.2 Tipos e Níveis de Certificado

Será abordado no texto abaixo, apesar deste conhecimento constar no curso de Nivelamento Teórico, os tipos e níveis de certificados que serão aceitos. É apenas uma orientação para a seqüência normal das explicações. Dentro das normas da ICP-BRASIL existem 2 (dois) tipos de certificado: Assinatura e Sigilo e cada um deles possui 4 níveis que são os seguintes:

De Assinatura:

A1: Chave criptográfica de 1024 bits gerada por software válida por 1 ano
- Trata-se de um arquivo geralmente com a extensão .pfx ou p12

A2: Chave criptográfica de 1024 bits gerada por hardware válida por 2 anos
- É um token ou SmartCard.

A3: Chave criptográfica de 1024 bits gerada por hardware válida por 3 anos
- É um token ou SmartCard.

A4: Chave criptográfica de 2048 bits gerada por hardware válida por 3 anos
- É um token ou SmartCard.

De Sigilo:

S1: Chave criptográfica de 1024 bits gerada por software válida por 1 ano

S2: Chave criptográfica de 1024 bits gerada por hardware válida por 2 anos

S3: Chave criptográfica de 1024 bits gerada por hardware válida por 3 anos

S4: Chave criptográfica de 2048 bits gerada por hardware válida por 3 anos

São as mesmas especificações que a do tipo Assinatura (An).

Por definição da ICP-BRASIL somente as chaves de Sigilo terão a cópia (backup) de segurança.

2 OBJETIVO

Este documento destina-se a orientar o portador (usuário) de certificados digitais, como também apoiar o atendimento (*help-desk / Central de Atendimento*) conforme o padrão ICP-BRASIL e de acordo com os requisitos esclarecidos anteriormente, deve funcionar como um guia para uso da certificação digital. O uso de outros tipos de certificados fora do padrão ICP-BRASIL não serão abordados neste documento, mas eventualmente muitos dos procedimentos podem valer para os mesmos.

3 AQUISIÇÃO OU RENOVAÇÃO DE CERTIFICADO DIGITAL PADRÃO ICP-BRASIL

Haverão casos em que o usuário ainda não possui um certificado ou o certificado expirou (perdeu a validade de acordo com o nível). Na hipótese do certificado estar expirado, a aplicação que está sendo utilizada pelo usuário, irá apontar este erro. Outra forma de se descobrir esta informação, é perguntar ao usuário se ele se lembra de quando fez o certificado e qual seria o tipo, assim é possível deduzir se o mesmo já expirou.

Nos itens a seguir estão os procedimentos para aquisição ou renovação de um certificado digital.

3.1 Aquisição

Para adquirir um certificado digital, independente do tipo, é obrigatório que o adquirente se dirija pessoalmente até uma Autoridade de Registro credenciada pela ICP-BRASIL. Pelas normas da ICP-BRASIL independente da autoridade de registro, os certificados terão a mesma validade e deverão ser aceitas por quaisquer aplicações que estejam no mesmo padrão, que é o caso das aplicações que utilizam a plataforma de desenvolvimento PINHÃO e o proto-agente TABELIÃO.

Para o processo de aquisição do certificado, os documentos necessários e obrigatórios são:

- ✔ Documento de identidade (RG).
- ✔ CPF.
- ✔ 2 (duas) fotos 3x4 recentes.
- ✔ Comprovante de residência recente (Menos de 3 meses).
- ✔ Dependendo da autoridade de registro outros documentos podem ser pedidos mas não são obrigatórios.

Será necessário apresentar uma cópia de cada um dos documentos acima, os quais serão anexados ao processo de certificação, e os documentos originais para comprovar a autenticidade.

O portador do certificado receberá o certificado (na mídia escolhida e conforme o tipo) e também uma cópia da política de certificado, que é uma espécie de contrato onde a pessoa assume as responsabilidades pelo porte do certificado. A validade do certificado varia conforme o seu tipo (item 1.2).

Uma recomendação muito IMPORTANTE é a definição de PIN (do inglês:*Personal Identification Number*) que é a senha do certificado, e PUK (do inglês: *Personal Unblocking Code*) que é a senha para desbloqueio do PIN caso necessário. Deve-se guardar bem estas senhas pois não será possível recuperá-las quando o certificado estiver em um Token ou SmartCard.

O procedimento formal para geração do certificado dependerá de cada Autoridade de Registro.

3.2 Renovação/Revalidação

De acordo com o tipo e nível, o certificado digital perderá sua validade após determinado período de tempo. Para renovar um certificado o usuário poderá fazê-lo presencialmente na autoridade de registro ou ainda através de um serviço disponibilizado na Internet por esta autoridade.

A renovação pela Internet só é possível se não houver nenhuma alteração dos dados com relação ao certificado anterior e por um número determinado de vezes, que no caso dos Tokens ou SmartCard são de 3 (três) vezes. Cada Autoridade Certificadora fornece este tipo de serviço em um endereço de Internet da própria Autoridade, estas informações e orientações devem ser checadas diretamente com a Autoridade.

A renovação presencial é feita no mesmo local (Autoridade de Registro) e forma como o certificado é adquirido.

Em ambos os casos é necessário estar de posse do Certificado no momento da renovação.

3.3 Revogação

Quando um certificado digital por algum motivo (esquecimento de senha, perda, roubo, extravio, desuso, etc...) precisa ser "cancelado" o procedimento e o termo utilizado é a **REVOGAÇÃO,** um certificado pode ser revogado junto à Autoridade Certificadora para que o mesmo perca a sua validade e uso mesmo antes do vencimento do prazo de validade.

A revogação pode ser feita através de um serviço "*on-line*" através de uma página Internet, disponibilizada pela Autoridade Certificadora, da mesma forma que o serviço de renovação. E, obviamente, também é possível ser feita a revogação de forma presencial diretamente na Autoridade de Registro.

Também é possível que por razões especiais (é abordado no curso de nivelamento teórico) a própria Autoridade Certificadora faça a revogação uni-literalmente.

Todos os certificados revogados constarão na Lista de Certificados Revogados (LCR) divulgada por cada Autoridade, e esta informação é validada pelo proto-agente TABELIÃO.

3.4 Importante

Somente para certificados de nível 1 (A1 e S1), armazenamento em arquivos, é possível obter-se uma "segunda via" do certificado, desde que tenha sido feito um procedimento de cópia *(backup)*. Portanto nos demais será necessário, em casos de extravio (inclusive da senha PIN), a emissão de um novo certificado.

4 FINALIDADES DE USO DOS CERTIFICADOS DIGITAIS

De posse de um certificado válido (dentro da validade e não-revogado) o seu portador (usuário) poderá utilizá-lo para usos específicos, abaixo listaremos os principais usos até o momento.

4.1 Assinatura Digital

Pode ser até considerada como principal uso de um certificado, a assinatura digital permite a identificação exata do autor de um documento eletrônico. Pode ser feita e validada através de uma aplicação que utilize a certificação digital. Pode ser utilizada para qualquer tipo de informação eletrônica.

4.2 Sigilo

São técnicas de criptografia que permitem que qualquer informação digital, seja codificada de forma que somente o proprietário da chave correspondente à operação de

decriptografia (decodificação), poderá ter acesso a esta informação.

4.3 Autenticação Segura

A autenticação segura é o já conhecido “login”, ou seja é a identificação precisa do usuário através do uso de um certificado digital. A principio qualquer sistema de informação, que utilize qualquer técnica de autenticação ou login, poderia substituí-lo pelo uso do certificado.

4.4 Principais softwares

Existem vários softwares que implementam a certificação digital, tanto proprietários como em software livre, abaixo serão listados alguns softwares do tipo livre:

4.4.1 Aplicações WEB/INTERNET

As aplicações desenvolvidas com o componente TABELIÃO-PINHÃO possuirão todas as capacidades da Certificação Digital. A maioria dos navegadores(Browser) de internet, possuem a capacidade de utilização das aplicações desenvolvidas com certificação digital.

Estão homologados através da GIC os navegadores baseados na tecnologia Mozilla, no documento *GIC_ManualConfiguracaoMozillaFirefox* são encontradas todas as informações para a configuração e uso.

4.4.2 Correio Eletrônico

A grande maioria dos software de correio eletrônico para desktop, já possuem as facilidades de assinatura e sigilo acopladas ao software. O software Mozilla-Thunderbird/Icedove foi homologado pela GIC e no documento *GIC_ManualConfiguracaoThunderbird* estão todas as informações necessárias para o seu uso.

4.4.3 Aplicativos Desktop

Existem iniciativas como a do ITI (www.iti.gov.br) que disponibiliza um aplicativo para uso em ambiente local (Desktop) e que permite o uso do certificado digital para as tarefas de assinatura e sigilo (criptografia). Tanto o software como as instruções de uso podem ser obtidas no site do ITI (www.iti.gov.br).

Há ainda o software que foi utilizado como base para o desenvolvimento do aplicativo do ITI que é o Cryptonit, este aplicativo assim como o do ITI foi homologado pela GIC e as orientações de uso estão no documento: *GIC_ManualCryptonit.* Este aplicativo possui versões

tanto para ambiente livre como proprietário, no caso do aplicativo do ITI somente para ambiente livre.

4.4.4 Pacotes (suites) de escritório.

O pacote ou *suite* de escritório open-office ou BR-Office(no Brasil) está preparada para efetuar assinaturas digitais nos seus principais programas que são o Writer, Calc e Impress. Esta funcionalidade foi testada e homologada pela GIC e trás no documento *GIC_ManualAssinaturaOpenOffice* as instruções detalhadas.

4.4.5 Apoio ao usuário.

Para todos os softwares homologados, além dos documentos referenciados, estão disponíveis no site da Plataforma PINHÃO (www.frameworkpinhao.pr.gov.br), vários vídeos (*screencast*) que podem apoiar no processo de aprendizagem.

Está disponível também o material para o curso de nivelamento teórico (apostila), um tutorial sobre certificação digital e as apresentações sobre o proto-agente TABELIÃO.

5 LISTA DE PERGUNTAS FREQÜÊNTES.

Neste item, em formato de lista de perguntas mais freqüentes (também conhecida como FAQ em inglês), serão abordadas as principais dúvidas e potenciais problemas que podem ocorrer durante o uso de certificado digitais.

5.1 Licenças de uso para softwares.

Nos manuais e recomendações da CELEPAR não é abordado o uso de softwares proprietários, assim, tanto as licenças, suporte ou as instruções de uso, devem ser adquiridas diretamente com o fornecedor do software ou a área responsável.

Nos casos dos aplicativos testados e homologados as licenças são de software livre, como GPL, Apache, etc... portanto não é necessário a obtenção ou pagamento de qualquer licença.

5.2 Onde conseguir Treinamentos.

A CELEPAR através da GIC (Gerência de Inovação Corporativa) oferece treinamentos para aquisição de conhecimento sobre Certificação Digital e o uso dos principais aplicativos testados e homologados.

5.3 Como Adquirir/receber o certificado?

A aquisição dos certificados é de responsabilidade do proprietário (usuário) que deverá fazê-lo pessoalmente em uma Autoridade Certificadora credenciada junto à ICP-BRASIL, mas o custo poderá ser de responsabilidade do órgão conforme as suas próprias determinações. Preferencialmente para os usuários que já concluíram o curso de nivelamento teórico oferecido pela GIC.

5.4 Já possui um certificado digital, pode utilizá-lo?

Caso o certificado que possui foi emitido por uma Autoridade Certificadora credenciada junto à ICP-BRASIL ele poderá ser utilizado por qualquer software ou aplicativo que siga este mesmo padrão. No caso das aplicações e sistemas homologados pela CELEPAR, através da GIC, elas estão neste padrão. O que poderá ocorrer é a aplicação exigir um nível de certificado maior, e nestes casos será necessária a aquisição do certificado neste nível. Já foi noticiado que algumas instituições bancárias pretendem oferecer certificados digitais ICP-BRASIL para seus clientes e portanto os mesmos poderão ser utilizados.

5.5 Quais os níveis de certificado são exigidos?

Os sistemas desenvolvidos especificamente para um determinado propósito, poderão exigir certificado de níveis variados conforme suas próprias exigências, e nestes casos os administradores dos sistemas é que definirão este nível.

Nos demais softwares de uso local (desktop) qualquer nível é aceito.

Veja também o item 1.2 deste manual.

5.6 Como adquirir certificado digital para uma aplicação.

A aquisição de um certificado para uma aplicação ou sistema é de responsabilidade do analista responsável por esta aplicação, e segue os mesmos padrões e exigências de um certificado de uso pessoal. Cada aplicação deverá possuir o seu próprio certificado, mesmo que estejam no mesmo servidor. Informações mais detalhadas a respeito da instalação deste tipo de certificado, pode ser obtida no documento: *GIC_CertificadosDigitaisAplicacoesWEB.*

5.7 O que são Token e SmartCard, quais são as suas diferenças?

Tanto os Tokens como os SmartCards (cartões inteligentes) possuem as mesmas propriedades e funcionalidades no que se referem a certificados digitais, pois são estes dispositivos que geram e armazenam as chaves criptográficas, ou seja a chave privada que ele armazena fica somente no dispositivo, que é protegida de forma absoluta contra violações.

Qualquer tentativa de violação (exportação, modificação) da chave privada não é permitida e a tentativa forçada pode levar à destruição da chave. Erros consecutivos da senha de acesso também poderão invalidar de forma irreversível a chave privada.

A principal diferença entre o Token e o SmartCard é que o Token pode ser inserido e lido diretamente da porta USB do computador, enquanto que o SmartCard precisa de uma leitora específica. O custo de um certificado em Token ou um SmartCard+Leitora é muito parecido, a escolha entre um ou outro dependerá da negociação com o fornecedor.

Ambos precisam de “Drivers” para seu funcionamento, no caso do ambiente Linux as bibliotecas são padrões e as instruções para a instalação e configuração destes estão no documento *GIC_ManualInstalacaoLeitoraseToken.* No caso de uso em ambiente proprietário, será necessário o suporte do fornecedor ou consulta aos manuais específicos.

5.8 A leitora de SmartCard ou Token não funcionam.

Em alguns casos ou mesmo em alguns momentos a Leitora ou o Token não são identificados pelo computador, nestes casos algumas providências podem ser tomadas:

1 – Consultar o documento *GIC_ManualInstalacaoLeitoraseToken.*

2 – Verificar se o led (sinal luminoso) do equipamento está piscando.

3 – Tentar utilizar em outra porta USB.

4 – Se possível testar em outro equipamento.

Se os problemas persistirem acionar o suporte da administração de equipamentos.

5.9 O certificado não está sendo reconhecido.

Caso a leitora/Token esteja funcionando perfeitamente mas o certificado não está sendo reconhecido verifique os seguinte itens:

1 – Consultar o documento *GIC_ManualInstalacaoLeitoraseToken.*

2 – O certificado foi emitido por AR da ICP-BRASIL?

3 – No caso de SmartCard: verificar a posição em que o cartão está inserido, pois o chip (circuito) deve estar voltado para cima.

4 – Cada aplicativo ou software que utiliza o certificado faz o bloqueio da leitora, portanto deverão ser utilizados separadamente, então verificar se não há nenhum outro software aberto,além daquele que se deseja utilizar, inclusive o navegador (browser) se não for este a ser utilizado. Após fechar todos os aplicativos deve-se retirar e reinserir o Token/SmartCard.

Se os problemas persistirem acionar o suporte.

5.10 O Sistema ou aplicativo avisa que a Lista de Certificado Revogado (LCR) está expirada.

As listas de certificados revogados têm uma data de validade e precisam ser atualizadas, a forma como cada aplicativo trata pode ser diferente portanto será necessária a consulta ao manual referente à ferramenta. Em ambientes com proxy alguns aplicativos não suportam e é necessária a inclusão da lista a partir de um arquivo, estes arquivos podem ser "baixados" diretamente do site da Autoridade Certificadora. Em aplicativos com o proto-agente TABELIÃO esta tarefa é feita automaticamente, nestes casos é preciso entrar em contato com a Central de Atendimento.

5.11 O Sistema avisa que o certificado não pode ser aceito.

Veja o item **Quais os níveis de certificado são exigidos.**

5.12 O Sistema avisa que o certificado é inválido.

Deve-se então verificar se o certificado é emitido por autoridade credenciada junto à ICP-BRASIL.

O Certificado não foi revogado?

Se possível testar em outro aplicativo.

5.13 O Sistema avisa que o certificado está expirando ou expirou.

Os sistemas que utilizam o TABELIÃO avisam quando o certificado está expirando e quando já expirou.

Quando ainda não expirou o usuário poderá acessar o sistema, mas deverá renovar o certificado o quanto antes.

Se o certificado expirou, dependendo do sistema o usuário poderá não ter acesso ao sistema ou terá acesso somente para consultas. Para resolver a situação o usuário deverá renovar o certificado.

A renovação é feita somente pelo usuário.

5.14 Perda ou esquecimento da senha pessoal (PIN) do certificado.

Se o certificado for dos níveis A1 ou S1 será possível obter uma outra cópia do certificado com a Autoridade de Registro.

Para os certificados de demais níveis não é possível a recuperação ou substituição da senha pois a mesma está armazenada somente no Token ou SmartCard. A primeira alternativa é o uso da senha PUK (também de propriedade do usuário) com esta senha é possível alterar o PIN.

Nos casos onde nenhuma das senhas é lembrada, a única solução é a emissão de um novo certificado junto com a revogação do antigo.

5.15 Modificar a senha pessoal (PIN)

Para fazer a modificação da senha do certificado, armazenada em um Token e SmartCard, bastará seguir as orientações de um dos seguintes manuais.

- *GIC_ManualInstalacaoLeitoraseToken:* No item 2.2.2 há instruções para alteração

da senha por meio de linha de comando no terminal (shell) do Linux.

- *GIC_ManualConfiguracaoThunderbird:* No item 5.5 há instruções para alteração da senha via interface gráfica do Leitor de E-mail Mozilla-Thuderbird e compatíveis.
- *GIC_ManualConfiguracaoMozillaFirefox:* No item 6.3 há instruções para alteração da senha via interface gráfica do Navegador(Browser) Mozilla-Firefox e compatíveis.

5.16 A senha pessoal (PIN) está bloqueada.

Para certificados em hardware (Token/Smartcard) é possível utilizar a senha PUK, para modificar a senha PIN.

No documento *GIC_ManualInstalacaoLeitoraseToken:* No item 2.2.3 há instruções para alteração da senha por meio de linha de comando no terminal (shell) do Linux.

5.17 Perdido ou extraviado o certificado digital.

Neste tipo de situação deve-se fazer a revogação imediata do certificado. Veja item 3.3 deste manual.

5.18 Algumas mensagens específicas do componente TABELIÃO-PINHÃO.

Em muitos casos algumas mensagens, ou mesmo interfaces(telas) que são enviadas pelos sistemas são na verdade oriundas do proto-agente TABELIÃO-PINHÃO e portanto seguem um mesmo padrão para estas mensagens e telas, adotando-se os seguintes procedimentos:

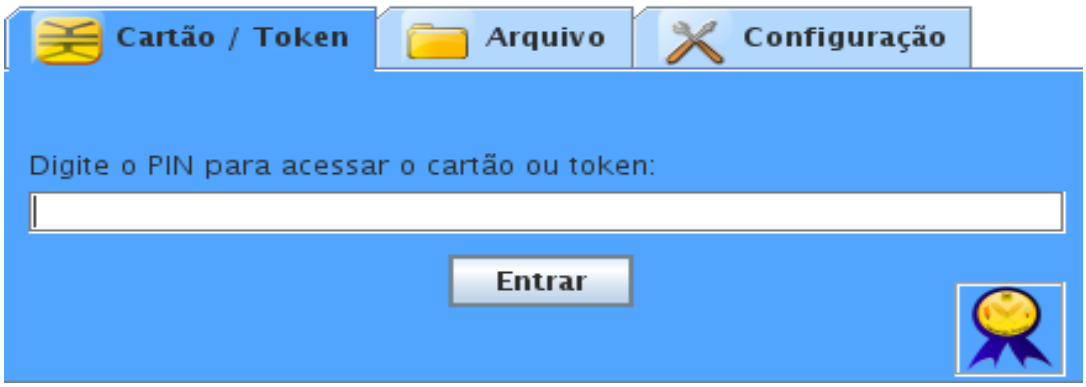

Figura 1. Aba/Tela para uso de certificado armazenado em Cartão/Token.

A figura 1 é apresentada quando é necessário uma leitura do certificado que está armazenado no Cartão(SmartCard) ou Token (níveis 3 e 4 ICP-BRASIL). Esta leitura é usada na Autenticação (login) ou quando é necessário efetuar uma assinatura digital.

Quando é selecionada a aba Cartão / Token a informação exigida é o PIN (senha pessoal).

Dependendo da configuração do sistema, uma ou outra aba não aparecerá, por exemplo: a aba Arquivo poderá aparecer sozinha.

No caso da aba Cartão/Token a aba configuração sempre aparecerá.

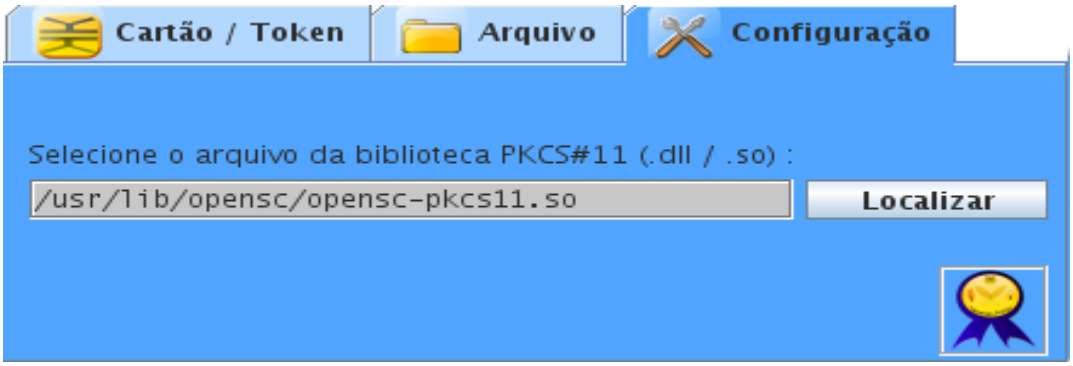

Figura 2. Aba/Tela de Configuração.

Esta aba é necessária somente quando o certificado utilizado está armazenado em Cartão (smartcard) ou Token, nela é possível indicar qual é a biblioteca que está sendo utilizada para leitura do dispositivo. (no Linux é sempre um arquivo .so)

Para selecionar entre Cartão/Token ou Arquivo é preciso clicar na aba correspondente seja **Cartão/Token** ou **Arquivo**.

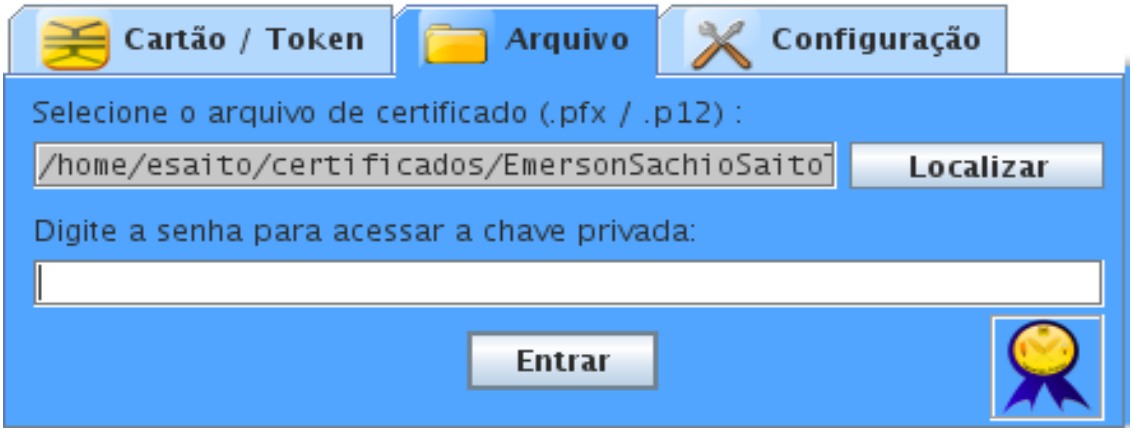

Figura 3. Aba/Tela para uso de certificado armazenado em arquivo.

Na aba Arquivo deverá ser informada a localização do arquivo com o certificado pessoal (normalmente com extensões .pfx ou .p12).

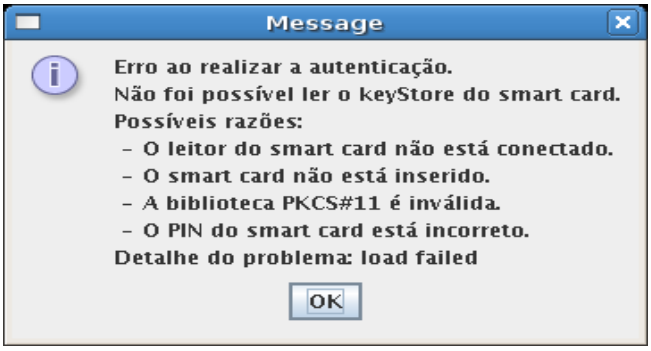

Figura 4. Mensagem de erro.

A Figura 4 é apresentada quando houver algum erro com relação ao certificado e os mais comuns são:

- A leitora ou Token não está conectado à entrada USB do computador: Verificar a entrada.
- O SmartCard não está inserido na leitora ou está inserido de forma incorreta: verificar o cartão e a posição de inserção com o chip para cima.
- No caso de certificado de software o local ou arquivo indicado é incorreto: verificar se o diretório corresponde e o arquivo é o correto.
- Para leitora ou Token: a biblioteca de software indicada pelo botão localizar não é válida: verificar se o diretório corresponde e o arquivo é o correto, no LINUX a extensão é .so.
- O PIN ou senha foi digitado incorretamente: verificar teclas como CapsLock ou NumLock além da senha correta.
- Para leitoras ou Token: caso o erro persista é possível que o problema possa estar na conexão USB, assim é um procedimento útil mudar a entrada(porta) que esta sendo utilizada.

6 CONSIDERAÇÕES FINAIS.

O objetivo deste documento é que a lista de perguntas freqüentes seja atualizada periodicamente conforme o uso e as necessidades.

Qualquer contribuição pode ser feita diretamente à GIC (Gerência de Inovação Corporativa) ou através do site da Plataforma PINHÃO (http://www.frameworkpinhao.pr.gov.br).