www.serpro.gov.br

# Guia de Integração


**Versão 1.9**
**Março de 2018**

SUNAF SERPRO

# Histórico de Versões

| Data | Descrição | Autor | Revisor | Aprovado por |
|---|---|---|---|---|
| 06/01/2017 | Versão inicial | Jorge Sena e Adriana Lima | | |
| 15/02/2017 | Adequações diversas | Helder Santos | Adriana Lima | |
| 17/03/2017 | Atualização dos URLs de solicitação de certificados | Helder Santos | Adriana Lima | |
| 19/09/2017 | Adaptação do guia à utilização do ambiente de Treinamento | Helder Santos | Greicy Rigo | |
| 06/03/2018 | Reordenação de Conteúdo e revisão de descritivos | Marcelo Leal | Greicy Rigo<br>Adriana Lima | |

# Sumário

1. Contextualização....4
2. Objetivo....4
3. Resumo dos passos para se integrar com o Sisdepen....6
4. Conhecer o Sisdepen Custodiado....10
5. Informações Técnicas....10
5.1. Tecnologias utilizadas....10
5.2. Ambientes disponíveis....11
5.3. Catálogo de Serviços....11
5.4. Segurança – Conexão com certificado digital....12
5.5. Bilhetagem na Integração....12
5.6. Usuários....13
5.7. Integridade de Dados e Transações....14
6. Processo de Integração – Resumo....14
7. Como o Sistema Externo se integra com o Sisdepen....15
7.1. Criar Certificado Digital de Equipamento....15
7.2. Solicitar Cadastro do Sistema Externo e Criação de Usuário....17
7.3. Testar Comunicação entre o Sistema Externo e o Sisdepen....18
8. Disposições Finais....18
9. Perguntas Frequentes....19
9.1. O certificado de produção tem que ser gerado pelo SERPRO?....19
9.2. Posso utilizar o certificado de uma pessoa física (e-CPF) ou uma pessoa jurídica (e-CNPJ) para cadastro no SISDEPEN?....19
9.3. Preciso criar um certificado para cada ambiente/servidor que eu for instalá-lo?....20
9.4. Posso utilizar um certificado autoassinado?....20
9.5. Quem gera o certificado de homologação?....20
9.6. O certificado de homologação pode ser usado na produção?....20
9.7. Após concluir o cadastro, o usuário tentou acessar o URL do WSDL do SISDEPEN e o navegador está solicitando login e senha ou então deu erro de handshake....20
10. Contatos....20
11. ANEXO I - Como gerar um certificado de Homologação [ Windows + Keystore explorer 5.0.1] ....21
11.1. Solicitar um certificado....21
11.2. Preparar o ambiente para geração do par de chaves....22
11.3. Gerar requisição para Autoridade de Registro (.CSR)....27
11.4. Instalar um certificado....28
11.5. Preparação e Montagem do certificado digital para utilização pela aplicação cliente....29
12. ANEXO II - Como gerar um certificado de Homologação [ Linux + OpenSSL]....34
12.1. Solicitar um certificado....34
12.2. Preparar o ambiente para geração do par de chaves....35
12.3. Gerar requisição para Autoridade de Registro (.CSR)....35
12.4. Instalar um certificado....36
12.5. Preparação e Montagem do certificado digital para utilização pela aplicação cliente....37
13. ANEXO III - Como gerar um certificado de Produção [ Windows + Keystore explorer 5.0.1]....38
13.1. Solicitar um certificado....38
13.2. Preparar o ambiente para geração do par de chaves....39
13.3. Gerar requisição para Autoridade de Registro (.CSR)....44
13.4. Instalar um certificado....46
13.5. Preparação e Montagem do certificado digital para utilização pela aplicação cliente....47
14. ANEXO IV - Como gerar um certificado de Produção [ Linux + OpenSSL] ....52
14.1. Solicitar um certificado....52
14.2. Preparar o ambiente para geração do par de chaves....53
14.3. Gerar requisição para Autoridade de Registro (.CSR)....53
14.4. Instalar um certificado....54
14.5. Preparação e Montagem do certificado digital para utilização pela aplicação cliente....55

## 1. Contextualização

O Sistema de Informações do Departamento Penitenciário Nacional – SISDEPEN é uma ferramenta fornecida pelo Ministério Extraordinário da Segurança Pública que visa ao cumprimento da Lei n° 12.714, de 14 de setembro de 2012.

A finalidade desta ferramenta é coletar informações padronizadas para um eficaz mapeamento do sistema penitenciário brasileiro. As informações coletadas estarão à disposição dos usuários para apoio à gestão prisional, formulação de políticas públicas e acompanhamento do cumprimento da pena privativa de liberdade, de prisão cautelar e da medida de segurança.

Devido à diversidade de soluções existentes nos estados e à carência de uma solução que unifique e padronize as informações a nível nacional, o SISDEPEN disponibiliza duas formas de inserção das informações; inserção manual dos dados por meio de utilização da interface web, a ser utilizada pelos estados que não possuem sistemas próprios e que passarão a utilizá-lo cadastrando diretamente as informações da estrutura organizacional e dos custodiados no sistema, e outra por meio do serviço de integração, onde será disponibilizada uma API – interface de programação de aplicativos – a ser utilizada pelos estados que possuem sistemas próprios e optam por mantê-los, passando a enviar os dados por meio dos serviços disponibilizados.

## 2. Objetivo

Este guia tem como objetivo fornecer orientações quanto aos procedimentos para integração com o SISDEPEN, apresentando o passo a passo e o funcionamento dos serviços (API's) do SISDEPEN, de modo a nortear os desenvolvedores dos estados que possuem sistema próprio, designado sistema externo, quanto às implementações necessárias à integração de seus sistemas e quanto à existência de um processo de solicitação ao DEPEN para integração, onde será apresentado o fluxo de demanda com seus papéis e responsabilidades.

Neste documento, apresentaremos o padrão disponibilizado pelo SISDEPEN para permitir as integrações. Trata-se da possibilidade de que potencialmente qualquer sistema se integre diretamente ao SISDEPEN através da troca de

mensagens.

Ao contrário da Integração via Arquivos Batch, este meio de integração tem reflexos imediatos no SISDEPEN, ou seja, qualquer requisição feita será processada e uma resposta será enviada ao sistema externo no mesmo momento. Outra característica é que este meio de integração está disponível apenas durante o período no qual o próprio sistema web está acessível ao usuário.

A natureza síncrona desta forma de integração a torna mais apropriada para sistemas que necessitem de uma comunicação interativa com o SISDEPEN.

## 3. Resumo dos passos para se integrar com o Sisdepen

# 01 Criar Certificado Digital de Equipamento

Para o estabelecimento de canal seguro para integração com o SISDEPEN, o sistema externo deverá possuir um certificado de Equipamento A1 assinado, preferencialmente, por uma das autoridades certificadoras (AC) da ICP-Brasil.

Caso o sistema externo já disponha de um certificado de equipamento A1 válido poderá utilizá-lo no processo de integração, sendo válida sua utilização nos ambientes de produção e treinamento.

Entretanto, se o órgão externo não possuir um certificado, com intuito de não onerar o Estado com a necessidade de aquisição prévia de um certificado digital para utilização desde o início do processo de integração, o Serpro disponibiliza uma opção para emissão de um certificado digital de testes a ser utilizado durante o desenvolvimento da integração com o Sisdepen e para realização de testes de integração utilizando o ambiente de Treinamento, ambiente destinado a esta fase.

O certificado de equipamento do tipo A1 tem validade de 1 ano. Assim, todo ano os sistemas externos precisarão renovar o certificado e enviar para o SISDEPEN de modo que ele passe a reconhecê-lo. Recomenda-se que o processo de renovação de certificado seja realizado nos últimos 30 (trinta) dias de validade do certificado atual, uma vez que após a expiração da validade do certificado o SISDEPEN passará a recusar a conexão do sistema externo.

## Criar Certificado Digital de Equipamento

Devido à diversidade de versões de sistemas operacionais e navegadores existentes, seguem orientações para a criação de um canal seguro por meio de autenticação mútua.

Certificado de Homologação
Windows + Keystore explorer 5.0.1
Guia de Integração - Pag. 21
Anexo I

Certificado de Produção
Windows + Keystore explorer 5.0.1
Guia de Integração - Pag. 40
Anexo III

Certificado de Homologação
Linux + OpenSSL
Guia de Integração - Pag. 36
Anexo II

Certificado de Produção
Linux + OpenSSL
Guia de Integração - Pag. 57
Anexo IV

# 02 Cadastro de Sistema Externo e Criação de Usuário

O sistema externo deverá ser cadastrado no SISDEPEN previamente para que o acesso aos serviços de integração seja possível, quando também será feita a opção do tipo de usuário a ser utilizado.

## Seguem maiores informações para cadastro do sistema e criação de usuário:

Informações necessárias a realização do cadastro do sistema externo:

- **Sigla do Sistema:** Alfanumérico até 16 caracteres, sem espaços
- **Nome do Sistema**: Alfanumérico até 100 caracteres
- **DN**: (Distinguished Name) do certificado do sistema. Opcionalmente, pode ser enviado o certificado (.cer), sem a sua senha, para extração/conferência do DN.
- **Tipo de autenticação:** Usuário Normal ou Usuário Especial (vide tópico 4.6 que detalha esses tipos de autenticação).

### Usuário Normal

O órgão providenciará o cadastro dos seus usuários no SISDEPEN nos respectivos sistemas e ambientes de destino (Produção e/ou Treinamento) por meio de seus cadastradores locais. Caso seu órgão não disponha de um cadastrador local, faz-se necessário o envio das requisições ao DEPEN.

Neste caso, o órgão externo deverá indicar ao DEPEN o usuário a ser utilizado.

### Usuário Especial

O órgão externo deverá enviar ao DEPEN:

- Termo de responsabilidade assinado pelo responsável pelo sistema externo;
- UF do sistema externo.

### Certificado Digital

O Sistema externo deverá encaminhar:

- Arquivo do certificado do sistema externo (.cer)

Obs.: Não é necessário o envio de senha do certificado.

# 03 Testar Comunicação

Após a confirmação de cadastro do certificado no SISDEPEN, o gestor do sistema externo deve efetuar teste de comunicação com o SISDEPEN. Para isso, sugerimos seguir os seguintes passos 1 e 2 abaixo:

O sistema externo é o responsável por realizar os controles necessários à garantia da integridade de dados e transações referentes à integração com o SISDEPEN. Problemas de comunicação, por exemplo, devem receber o devido tratamento, a fim de evitar distorções tanto no sistema externo quanto no SISDEPEN.

## 1 Importar no navegador o arquivo '.pfx' ou '.p12'

o arquivo '.pfx' ou '.p12' (PKCS #12) que possui as chaves pública, privada e cadeias da autoridade certificadora que assinou o certificado. O arquivo '.pfx' ou '.p12' define um formato para armazenar vários objetos de criptografia em um único arquivo. Para realizar a importação no navegador, o usuário deve acessar a área de criptografia do navegador e importar o arquivo '.pfx' ou '.p12' em 'seus certificados'.

Para os testes de comunicação, o SISDEPEN recomenda a utilização do navegador Mozilla Firefox. Para importar o arquivo (ref. Firefox v51):

**Menu --> Opções --> Avançado --> Certificados --> Ver certificados --> Seus certificados --> Importar**

## 2 Acessar a URL do WSDL do SISDEPEN para o

Siga as instruções conforme descrito nos seguintes documentos:

- **Documentação de Serviços de Interoperabilidade – Tabelas Administrativas. (SISDEPEN-PIE-WebServices-Tabelas-Administrativas.pdf**
  **SISDEPEN - Documentação de Serviços de Interoperabilidade – Custodiado. (SISDEPEN-PIE-WebServices-Custodiado.pdf)**

Os documentos acima encontram-se em
*http://depen.gov.br/DEPEN/sisdepen/download/download*

Caso o WSDL seja aberto pelo navegador, o cadastro foi realizado com sucesso.

## 4. Conhecer o Sisdepen Custodiado

O desenvolvedor responsável pela integração com o Sisdepen necessita de ter uma visão de negócio do módulo custodiado, seu objetivo e os conceitos envolvidos, para melhor entendimento da documentação técnica do serviço de integração. Para tanto, estão disponíveis o Tutorial e o Manual do Usuário – http://depen.gov.br/DEPEN/depen/sisdepen/sisdepen no sítio do DEPEN – Departamento Penitenciário Nacional.

## 5. Informações Técnicas

As informações e configurações descritas neste tópico são essenciais ao correto funcionamento da integração. Para viabilizar a integração de sistemas externos ao SISDEPEN, os responsáveis pelos sistemas externos devem observar os tópicos a seguir.

### 5.1. Tecnologias utilizadas

A oferta de serviços do SISDEPEN via *webservices* se fundamenta basicamente em duas tecnologias:

- Simple Object Access Protocol (SOAP): protocolo baseado em XML. Permite que os clientes se comuniquem com os provedores de serviço;
- Web Services Description Language (WSDL): define a interface de acesso ao serviço.

Independentemente da tecnologia escolhida para implementação da integração do sistema externo com os serviços do SISDEPEN, os gestores dos sistemas externos que desejam se integrar devem ter domínio sobre o uso das tecnologias listadas acima.

Todos os serviços ofertados pelo SISDEPEN estão aderentes à arquitetura e-PING (Padrões de Interoperabilidade de Governo Eletrônico), que define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) no governo federal, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral.

## 5.2. Ambientes disponíveis

Os ambientes abaixo estão disponíveis para os sistemas externos se integrarem com o SISDEPEN.

| Ambiente | Endereço | Disponibilidade | Objetivo |
|---|---|---|---|
| Treinamento | Disponível no catálogo de serviços. Ver item 4.3. | Segunda a sexta, 08:00 às 18:00 | Ambiente que dispõe da última versão de software implantada em produção. Faz uso de dados fictícios. |
| Produção | | 24 horas, 7 dias por semana | Ambiente que possui a versão de software e dados oficiais do serviço. |

Cada estado precisará adequar seus sistemas de modo a ter uma interface de comunicação com o Sisdepen, por meio de webservices (API's).

A equipe do sistema externo fará uso do ambiente de treinamento do SISDEPEN para execução dos testes de integração. O ambiente de treinamento está disponível na internet e dispensa a necessidade de liberação de rede específica para ser acessado.

O ambiente de treinamento não poderá ser utilizado para a realização de testes de requisitos não funcionais (performance ou carga).

O acesso aos ambientes do SISDEPEN seguem a sequência de utilização, sendo concedido primeiro o acesso ao ambiente de treinamento e depois ao ambiente de produção.

O cadastro no ambiente de produção poderá ser realizado após a homologação da integração junto ao DEPEN.

## 5.3. Catálogo de Serviços

Para que os sistemas externos estabeleçam uma conexão via webservice com o SISDEPEN, seus respectivos gestores devem consultar os seguintes documentos:

- SISDEPEN - Documentação de Serviços de Interoperabilidade – Tabelas Administrativas (SISDEPEN-PIE-WebServices-Tabelas-Adminiatrativas.pdf);
- SISDEPEN - Documentação de Serviços de Interoperabilidade – Custodiado (SISDEPEN-PIE-WebServices-Custodiado.pdf).

A referida documentação se encontra disponível no sítio do DEPEN, no endereço: http://depen.gov.br/DEPEN/depen/sisdepen/download/download

A oferta de serviços é ampla, mas não abrange todas as funcionalidades do SISDEPEN. Entretanto, em havendo necessidade de evolução, poderá ser encaminhada solicitação ao DEPEN.

## 5.4. Segurança – Conexão com certificado digital

Para estabelecimento de uma conexão segura entre o SISDEPEN e um sistema externo, faz-se necessário o estabelecimento de uma autenticação mútua entre os sistemas, a fim de criar um canal seguro para a troca de mensagens. Esta autenticação mútua é realizada por meio do cadastro prévio do certificado digital do sistema externo dentro do SISDEPEN, onde o protocolo HTTPS é utilizado para efetuar transações on-line seguras.

Para o estabelecimento desse canal seguro, o sistema externo precisará de um certificado de Equipamento A1 assinado, preferencialmente, por uma das autoridades certificadoras (AC) da ICP-Brasil.

Caso o sistema externo já disponha de um certificado de equipamento A1 poderá utilizá-lo, caso contrário, poderá fazer uso de um certificado digital de testes disponibilizado pelo Serpro. Maiores informações serão apresentadas no item 6.1. Criar Certificado Digital de Equipamento.

## 5.5. Bilhetagem na Integração

Qualquer sistema externo devidamente habilitado pode enviar mensagens SOAP para a interface do SISDEPEN. Estas mensagens, se estiverem consistentes com a especificação de interface publicada, serão processadas e respondidas.

Para evitar que problemas de rede resultem em duplicidade de requisições, as mensagens passam por controle de bilhetagem. O SISDEPEN não aceita o reenvio da mesma requisição para alterar a base do sistema. Requisições de consulta não sofrem este tipo de restrição.

Maiores informações sobre o funcionamento dos serviços estão disponíveis no catálogo de serviço.

## 5.6. Usuários

A autenticação do sistema externo com o SISDEPEN é realizada via *webservice,* e pode ser feita de duas formas:

**Usuário especial:** é aquele o qual o usuário criado será vinculado ao Gestor responsável do serviço no órgão, e a senha utilizada por esse usuário não é uma senha pessoal e sim a senha do certificado digital, que identifica o sistema externo em vez de um indivíduo.
Este usuário será identificado por um código no seguinte formato: **ZZXXXXXNNNN** (ZZ = UF, XXXXX = Código da EO, NNNN = número sequencial).
A criação deve ser solicitada ao DEPEN mediante preenchimento de termo de responsabilidade, o qual identificará a pessoa responsável pelo sistema que se integrará com o SISDEPEN.

**Usuário normal:** é aquele usuário cujo cadastro utiliza seu CPF e senha pessoal. Esse cadastrado é realizado pelo cadastrador de seu órgão através das funcionalidades: Pré-cadastro e Primeiro Acesso. O cadastrador efetuará o pré-cadastro do usuário com informações essenciais e determinando o perfil de acesso, o qual possibilitará ao usuário a fazer o primeiro acesso, onde complementará os dados de seu cadastro e criará a sua senha pessoal.
Para a criação de usuário normal no Sisdepen, o órgão providenciará seu cadastro por meio dos seus Cadastradores Locais, nos respectivos sistemas e ambientes de destino (Treinamento e/ou Produção). Caso o seu órgão não disponha de um cadastrador local, faz-se necessário o envio das requisições ao DEPEN.

Importante ressaltar que a concessão de acesso a cada um dos ambientes (Treinamento e Produção) é feita separadamente e o usuário deverá solicitá-lo para os sistemas/módulos aos quais necessite de acesso.

Cada mensagem emitida pelo sistema externo deverá conter os dados de autenticação de um usuário habilitado no SISDEPEN. Dessa forma, todas as requisições serão associadas a um usuário com CPF ou a um usuário especial no SISDEPEN.

## 5.7. Integridade de Dados e Transações

O sistema externo é o responsável por realizar os controles necessários à garantia da integridade de dados e transações referentes à integração com o SISDEPEN. Problemas de comunicação, por exemplo, devem receber o devido tratamento, a fim de evitar distorções tanto no sistema externo quanto no SISDEPEN.

O único meio de recuperação de um custodiado para detalhamento, alteração ou movimentação no SISDEPEN via *webservice* é por meio do CNC (código de identificação gerado pelo SISDEPEN). Portanto, o sistema externo deverá armazenar este código para manutenção do registro enviado ao SISDEPEN por integração.

## 6. Processo de Integração – Resumo

1) O órgão externo:

1.1) Comunica ao DEPEN o interesse na integração.

2) O DEPEN:

2.1) Avalia a pertinência da solicitação e autoriza sua integração.

3) O órgão externo:

3.1) Solicita autorização acompanhado do envio das informações necessárias – ver item “6.2” deste guia;

3.2) Caso o órgão não tenha certificado digital, solicita emissão de certificado digital de testes (para certificado de Homologação ver item “6.1.” deste guia).

4) O DEPEN:

4.1) Avalia a pertinência da solicitação e autoriza sua integração;

4.2) Obtém junto ao órgão externo as informações necessárias para solicitar cadastro de sistema externo e criação de usuário Sisdepen. Ver item “6.2.” deste guia;

4.3) Caso o órgão não tenha enviado o certificado digital, o DEPEN orienta a emissão de certificado digital de testes (para certificado de Homologação ver item “6.1.” deste guia) e aguarda a emissão pelo órgão;

4.4) Abre demanda do tipo “Apoio” para o SERPRO com as informações necessárias encaminhadas pelo órgão externo para liberação de acesso ao ambiente requerido.

5) O SERPRO realiza o atendimento da demanda e comunica ao DEPEN;

6) O DEPEN comunica ao órgão externo;

7) O órgão externo:

7.1) Testa a comunicação entre seu sistema com o Sisdepen e comunica ao DEPEN. Ver item “6.3” deste guia;

7.2) Realiza adequações no seu sistema;

7.3) Utiliza o ambiente de Treinamento do Sisdepen para testar a integração dele com o seu sistema;

7.4) Homologa as adequações realizadas no seu sistema;

7.5) Comunica ao DEPEN a conclusão do desenvolvimento e a homologação das adequações.

**Importante:** Esse passos deverão ser executados para cada ambiente do Sisdepen (Treinamento e Produção).

## 7. Como o Sistema Externo se integra com o Sisdepen

### 7.1. Criar Certificado Digital de Equipamento

Para o estabelecimento de canal seguro para integração com o SISDEPEN, o sistema externo deverá possuir um certificado de Equipamento A1 assinado, preferencialmente, por uma das autoridades certificadoras (AC) da ICP-Brasil.

Caso o sistema externo já disponha de um certificado de equipamento A1 válido poderá utilizá-lo no processo de integração, sendo válida sua utilização nos ambientes de produção e treinamento.

Entretanto, se o órgão externo não possuir um certificado, com intuito de não onerar o Estado com a necessidade de aquisição prévia de um certificado digital para utilização desde o início do processo de integração, o Serpro disponibiliza uma opção para emissão de um certificado digital de teses a ser utilizado durante o desenvolvimento da integração com o Sisdepen e para realização de testes de integração utilizando o ambiente de Treinamento, ambiente destinado a esta fase.

O ambiente de produção do Sisdepen requer um certificado digital de equipamento A1 assinado e válido, sendo um pré-requisito para seu pleno funcionamento. Para esse ambiente não existe opção de certificado de testes

sendo um ônus do órgão externo.

Apresentamos a seguir os roteiros padrões para a emissão de certificado digital de equipamento para integração com o Sisdepen. Tais roteiros devem ser entendidos como orientações para a criação de um canal seguro por meio de autenticação mútua.

Devido à diversidade de versões de sistemas operacionais e navegadores existentes, os roteiros podem não representar fielmente as versões que o desenvolvedor utiliza. Dessa forma, não se deve ficar preso ao que está descrito nos roteiros, que servem apenas como uma referência para nortear essa atividade.

- **Certificado de Homologação:** (utilizado para acesso ao ambiente de Treinamento do SISDEPEN)
  - ANEXO I - Como gerar um certificado de Homologação [ Windows + Keystore explorer 5.0.1]
  - ANEXO II - Como gerar um certificado de Homologação [ Linux + OpenSSL]

- **Certificado de Produção:** (utilizado para acesso ao ambiente de Produção do SISDEPEN).
  - ANEXO III - Como gerar um certificado de Produção [ Windows + Keystore explorer 5.0.1]
  - ANEXO IV - Como gerar um certificado de Produção [ Linux + OpenSSL]

**Importante:**

O certificado de equipamento do tipo A1 tem validade de 1 ano. Assim, todo ano os sistemas externos precisarão renovar o certificado e enviar para o SISDEPEN de modo que ele passe a reconhecê-lo. Recomenda-se que o processo de renovação de certificado seja realizado nos últimos 30 (trinta) dias de validade do certificado atual, uma vez que após a expiração da validade do certificado o SISDEPEN passará a recusar a conexão do sistema externo.

## 7.2. Solicitar Cadastro do Sistema Externo e Criação de Usuário

O sistema externo deverá ser cadastrado no SISDEPEN previamente para que o acesso aos serviços de integração seja possível, quando também será feita a opção do tipo de usuário a ser utilizado.

Informações necessárias a realização do cadastro do sistema externo

- **Sigla do Sistema:** Alfanumérico até 16 caracteres, sem espaços
- **Nome do Sistema:** Alfanumérico até 100 caracteres
- **DN:** (Distinguished Name) do certificado do sistema. Opcionalmente, pode ser enviado o certificado (.cer), sem a sua senha, para extração/conferência do DN.
- **Tipo de autenticação**: Usuário Normal ou Usuário Especial (vide tópico 4.6 que detalha esses tipos de autenticação).
  O Depen avaliará a solicitação do sistema para autenticação com Usuário Especial (sem senha).

Seguem maiores informações para cadastro do sistema e criação de usuário:

a) Para a criação de Usuário Normal, o órgão providenciará o cadastro dos seus usuários no SISDEPEN nos respectivos sistemas e ambientes de destino (Produção e/ou Treinamento) por meio de seus cadastradores locais. Caso seu órgão não disponha de um cadastrador local, faz-se necessário o envio das requisições ao DEPEN.

   Neste caso, o órgão externo deverá indicar ao DEPEN o usuário a ser utilizado.

b) Para a criação de Usuário Especial, caso seja este o "Tipo de autenticação" escolhido, o órgão externo deverá enviar ao DEPEN:
   - Termo de responsabilidade assinado pelo responsável pelo sistema externo;
   - UF do sistema externo.

   Neste caso, o órgão externo deverá indicar a opção desejada e o DEPEN definirá as seguintes informações:
   - EO para vínculo ao usuário especial;
   - Perfil para vínculo ao usuário especial.

c) Para o cadastro de certificado digital de sistema externo é necessário encaminhar:
   - Arquivo do certificado do sistema externo (.cer)

   Obs.: **Não** é necessário o envio de senha do certificado.

## 7.3. Testar Comunicação entre o Sistema Externo e o Sisdepen

Após a confirmação de cadastro do certificado no SISDEPEN, o gestor do sistema externo deve efetuar teste de comunicação com o SISDEPEN. Para isso, sugerimos seguir os seguintes passos:

1 - Importar no navegador o arquivo '.pfx' ou '.p12' (PKCS #12) que possui as chaves pública, privada e cadeias da autoridade certificadora que assinou o certificado. O arquivo '.pfx' ou '.p12' define um formato para armazenar vários objetos de criptografia em um único arquivo. Para realizar a importação no navegador, o usuário deve acessar a área de criptografia do navegador e importar o arquivo '.pfx' ou '.p12' em 'seus certificados'.

Para os testes de comunicação, o SISDEPEN recomenda a utilização do navegador Mozilla Firefox. Para importar o arquivo (ref. Firefox v51):

Menu → Opções → Avançado → Certificados → Ver certificados → Seus certificados → Importar.

Por fim, basta informar a senha do arquivo '.pfx' ou '.p12'.

2 - Acessar a URL do WSDL do SISDEPEN para o ambiente desejado, conforme descrito nos seguintes documentos:

- Documentação de Serviços de Interoperabilidade – Tabelas Administrativas.

  (SISDEPEN-PIE-WebServices-Tabelas-Administrativas.pdf

- SISDEPEN - Documentação de Serviços de Interoperabilidade – Custodiado. (SISDEPEN-PIE-WebServices-Custodiado.pdf)

Caso o WSDL seja aberto pelo navegador, o cadastro foi realizado com sucesso. Caso contrário, será necessário entrar em contato com o DEPEN para análise do problema.

## 8. Disposições Finais

- A documentação de API disponibilizada neste artefato está relacionada à integração via *webservices*. Necessidade de outro tipo de integração, não

contemplada neste artefato ou que requeira adequação, deverá ser negociada com o DEPEN.

- Os testes de conexão de que trata este documento dizem respeito aos testes de funcionamento da aplicação sob aspectos funcionais da integração entre os sistemas.
- Os testes de requisitos não funcionais devem ser objeto de demanda específica a ser efetuada ao DEPEN e requerem um planejamento para sua realização, bem como a disponibilidade de ambiente específico para sua execução. O ambiente de treinamento não deve ser utilizado para a realização desta atividade.
- As mudanças de infraestrutura nos ambientes produtivos do Sisdepen, as atualizações das versões de software e as mudanças físicas ou lógicas que venham a afetar o serviço serão acordadas previamente com os envolvidos por meio do DEPEN.
- Na medida do possível, pedimos que os marcos de implantação de uma integração com o SISDEPEN sejam informados ao Serpro, com o intuito de realizar uma monitoração proativa dos ambientes produtivos.

## 9. Perguntas Frequentes

### 9.1. O certificado de produção tem que ser gerado pelo SERPRO?

Não. O certificado digital emitido deve conter cadeias de homologação ou oficiais para os ambientes de Treinamento e de Produção do SISDEPEN. O certificado de equipamento deverá ser do tipo A1 e assinado, preferencialmente, por uma autoridade certificadora da ICP-Brasil.

### 9.2. Posso utilizar o certificado de uma pessoa física (e-CPF) ou uma pessoa jurídica (e-CNPJ) para cadastro no SISDEPEN?

Não. A exigência é que seja um certificado de equipamento do tipo A1, assinado preferencialmente por uma autoridade certificadora da ICP-Brasil.

### 9.3. Preciso criar um certificado para cada ambiente/servidor que eu for instalá-lo?

Não. Apesar de ter o nome de “certificado de equipamento”, o certificado é vinculado ao DNS da aplicação e poderá ser utilizado em mais de um servidor, desde que seja para a mesma aplicação.

### 9.4. Posso utilizar um certificado autoassinado?

Não. O certificado digital emitido deve conter cadeias de homologação ou oficiais para os ambientes de Treinamento e de Produção do SISDEPEN. O certificado de equipamento deverá ser do tipo A1 e assinado, preferencialmente, por uma autoridade certificadora da ICP-Brasil.

### 9.5. Quem gera o certificado de homologação?

O certificado de homologação poderá ser gerado pelo Serpro, sem custo para o DEPEN ou para o sistema externo, e destina-se a realização de testes.

### 9.6. O certificado de homologação pode ser usado na produção?

Não. O certificado de homologação funciona apenas no serviço de homologação ou para realização de testes.

### 9.7. Após concluir o cadastro, o usuário tentou acessar o URL do WSDL do SISDEPEN e o navegador está solicitando login e senha ou então deu erro de handshake.

Algum problema aconteceu no cadastramento do certificado digital. Gentileza acionar o DEPEN para análise do problema.

## 10. Contatos

| MINISTÉRIO EXTRAORDINÁRIO DA SEGURANÇA PÚBLICA | | | |
|---|---|---|---|
| **Nome** | **Papel** | **Telefone** | **e-mail** |
| Lucas Eneas de Rezende | - | (61) 2025-9978 | sisdepen@mj.gov.br |
| Hugo Romero Fernandes Devoti | - | | |

# 11. ANEXO I - Como gerar um certificado de Homologação [Windows + Keystore explorer 5.0.1]

## 11.1. Solicitar um certificado

1 Acessar o site: https://certificadoshom.serpro.gov.br/arserprossl/;

2 Navegar no seguinte fluxo: **'Meu Certificado -> Solicitar -> Equipamento'**;

**2.1** Acionar o link **'Equipamento A1 (Institucional)'** caso o seu Órgão tenha contrato com o SERPRO para emissão de certificados;

**2.2** Acionar o link **'Certificado de Equipamento A1 - R$ XXX,XX'** caso o seu Órgão não tenha contrato com o SERPRO para emissão de certificados;

3 Preencher o Formulário de Solicitação para Certificado Digital - Equipamento A1;

**3.1** No campo **'* URL'** preencher com o DNS ou Nome da aplicação. O usuário não poderá usar o caractere barra "/" neste campo;

4 Após finalizada a solicitação o sistema irá exibir informações detalhadas dos procedimentos adicionais que deverão ser realizados para a emissão do Certificado Digital.

**4.1** Envie um e-mail para o endereço certificados-homologacao-sisdepen@serpro.gov.br com o seguinte texto:

> Solicito a geração de certificado digital para testes.
>
> **Número de Referência do Pedido:** <numero>
> **Tipo de Certificado:** Equipamento A1
> **Ambiente da Solicitação:** https://certificadoshom.serpro.gov.br/arserprossl/
> **Sistema:** <sistema>

**4.1.1** <numero> é o número da solicitação obtido no *passo 4 deste tópico*;

**4.1.2** <sistema> é o nome do sistema a ser integrado com o SISDEPEN informado no campo **'* URL'.**

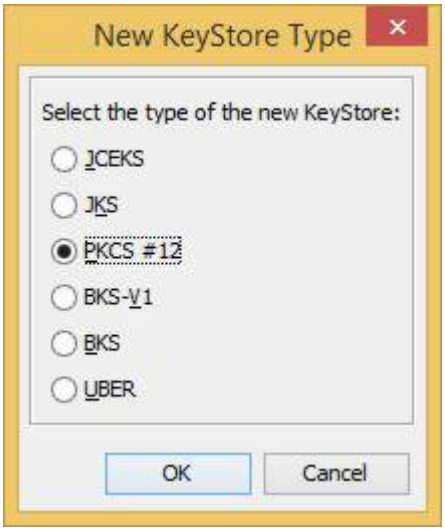
## 11.2. Preparar o ambiente para geração do par de chaves

Observação: As instruções a seguir foram baseadas em um ambiente Windows com o programa Keystore Explore 5.0.1

**Dica 1:** Realize todo o processo em uma mesma máquina/servidor.
**Dica 2:** Se você não tem familiaridade com este processo, crie uma senha única para informar sempre que for solicitado.
**Dica 3:** Crie senhas com caracteres especiais e números.

1 Abra o KeyStore Explorer e selecione a opção "Create a new KeyStore":

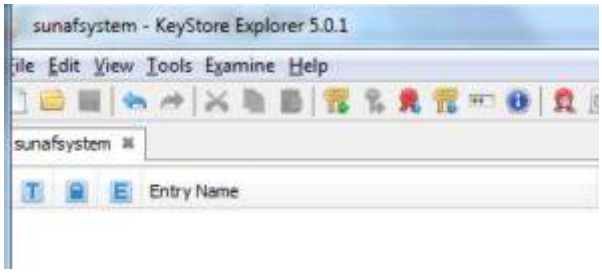
2 Faça o download do keyStore Explorer em http://keystore-explorer.sourceforge.net/downloads.php;

3 Salve a keystore com o nome do seu sistema:


4 O programa irá te solicitar uma senha para este keystore:

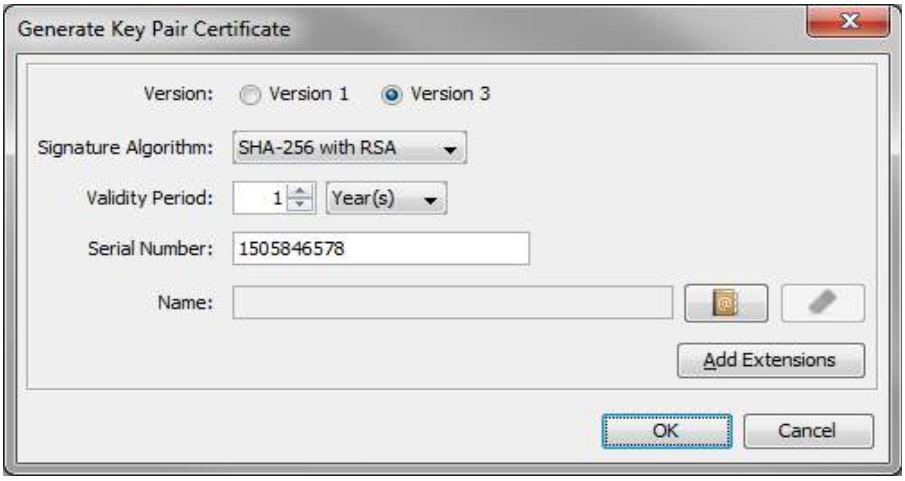
5 Observe que o Keystore (Nome da Aba) foi criado com o nome informado:




6 Acione o botão de geração do par de chaves::

7 Informe o algoritmo 'RSA' e o tamanho da chave '2.048':


8 Informe a **versão 3**, o algoritmo de assinatura **'SHA-256 with RSA'**, 1 ano de validade:

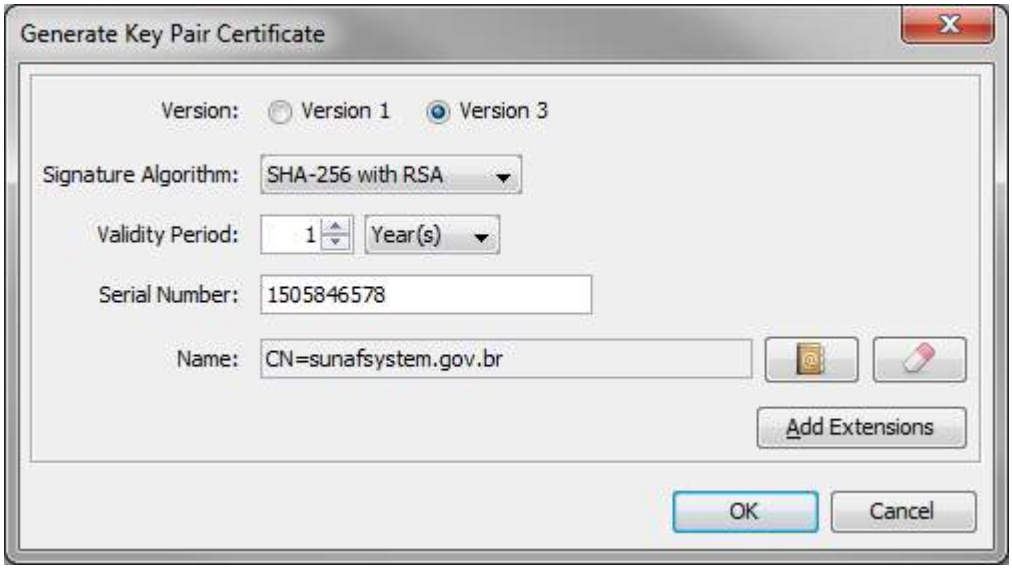


9 Edite o Nome do certificado acionando o botão 'Edit name':


10 A **única** informação necessária para a Autoridade de Registro do SERPRO é o campo **'Common Name (CN):'** que deverá ser preenchido com a mesma informação adicionada no campo **'* URL'** do Formulário de Solicitação para Certificado Digital - Equipamento A1. Os demais campos deixar em branco:

**Obs: o usuário não poderá usar o caractere barra "/" no CN**


11 Selecione 'OK' e verifique que no campo 'Name' terá apenas a informação 'CN=<sistema>':

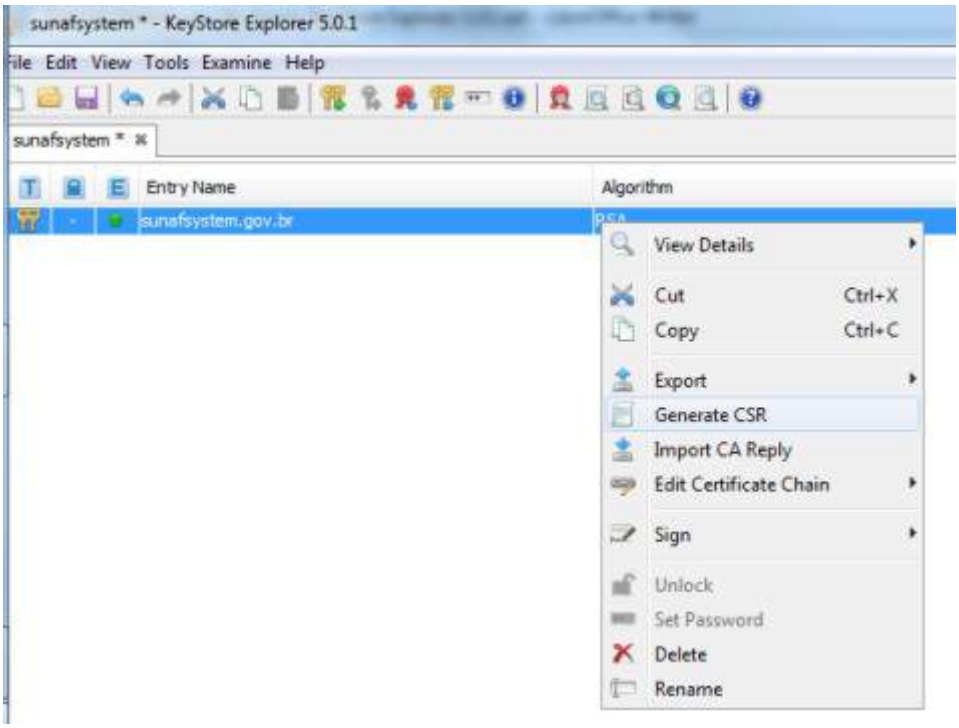



12 Selecione 'OK' e o sistema irá solicitar um alias para o par de chaves a ser gerado. Informe a mesma informação adicionada no campo **'* URL'** do Formulário de Solicitação para Certificado Digital - Equipamento A1:


13 Confirme e o sistema exibirá uma mensagem de sucesso na geração do par de chaves:

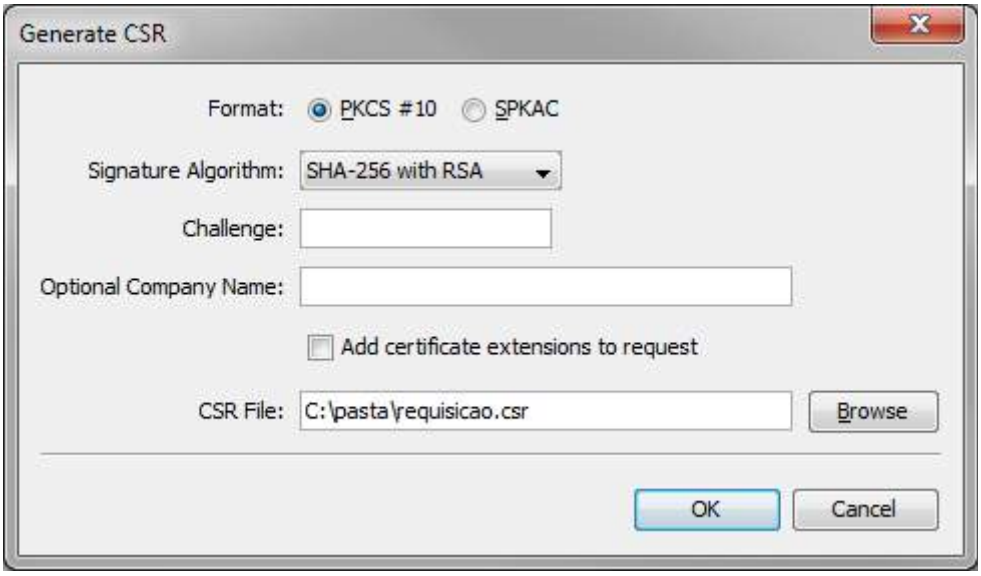
## 11.3. Gerar requisição para Autoridade de Registro (.CSR)

1 Clique com o botão direito sobre a keystore e acione a opção 'Generate CSR' para gerar a requisição a ser informada no momento da instalação do certificado no site da Autoridade de Registro **'requisicao.csr'**:




2 Informe como parâmetros para o arquivo CSR os seguintes valores:

- 2.1 Format: **PKCS #10**;
- 2.2 Signature Algorithm: **SHA-256 with RSA**;
- 2.3 Challenge: **(Deixe em branco)**;
- 2.4 CSR File: **'requisicao.csr'**




3 Após a execução do *passo 2 deste tópico*, será gerado o arquivo **'requisicao.csr'** com o conteúdo a ser informado no site da Autoridade de Registro no momento da instalação;

4 Aguarde o e-mail da Autoridade de Registro informando que o seu certificado está aprovado.


## 11.4. Instalar um certificado

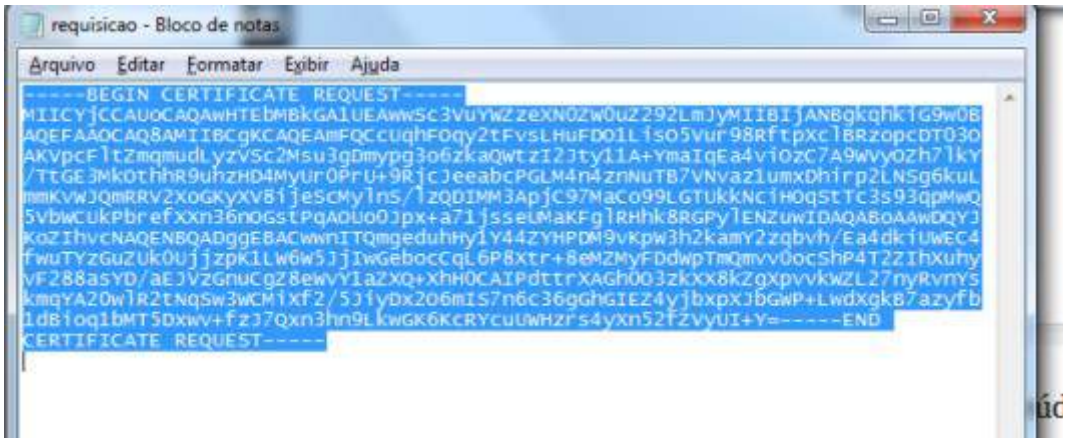
1 Uma vez que a solicitação de certificado já foi aprovada por uma Autoridade de Registro (A Autoridade de Registro envia um e-mail informando a aprovação), o último passo para a obtenção do Certificado Digital é a instalação.

2 Acessar o site: https://certificadoshom.serpro.gov.br/arserprossl/;

3 Acessar o menu **"Meu Certificado → Baixar"**

3.1 Neste ponto o solicitante deverá apresentar suas credenciais de acesso e em seguida será apresentada a tela para instalação/download do seu Certificado Digital.

4 Na tela de instalação do certificado, informar no único campo texto da tela o conteúdo do arquivo gerado no *passo 2.4 do tópico Gerar requisição para Autoridade de Registro (.CSR)* e acione o botão **'Salvar Certificado'**;




5 O site disponibilizará um arquivo com o nome do URL informada e extensão .p7b '**<sistema>.p7b**'. Este arquivo contém a sua chave pública assinada e a cadeia confiável da Autoridade de Registro. Salve-o em seu computador e por segurança faça uma cópia de backup.

## 11.5. Preparação e Montagem do certificado digital para utilização pela aplicação cliente

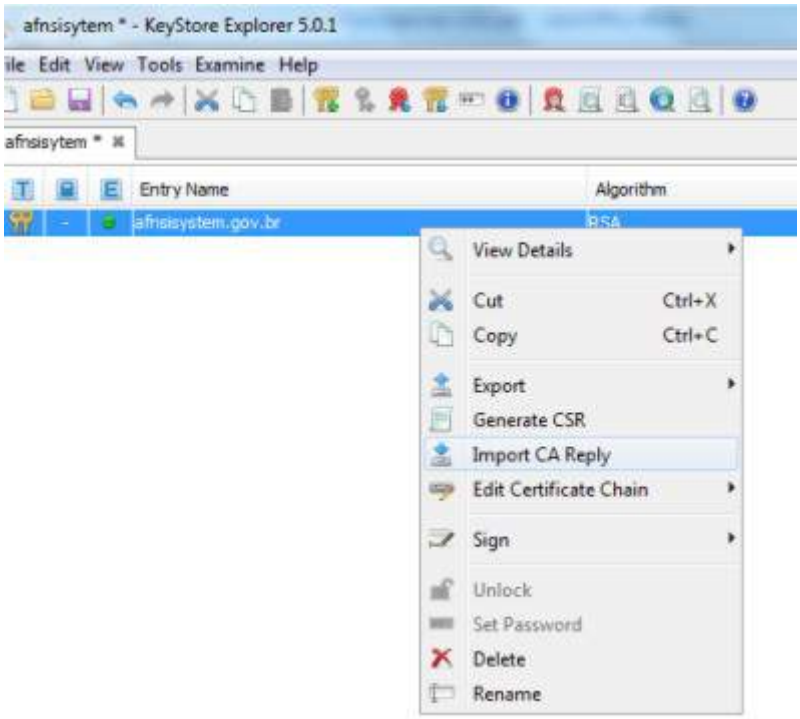
1 Converta o arquivo .p7b para o formato PEM que é reconhecido pelo KeyStore Explorer.

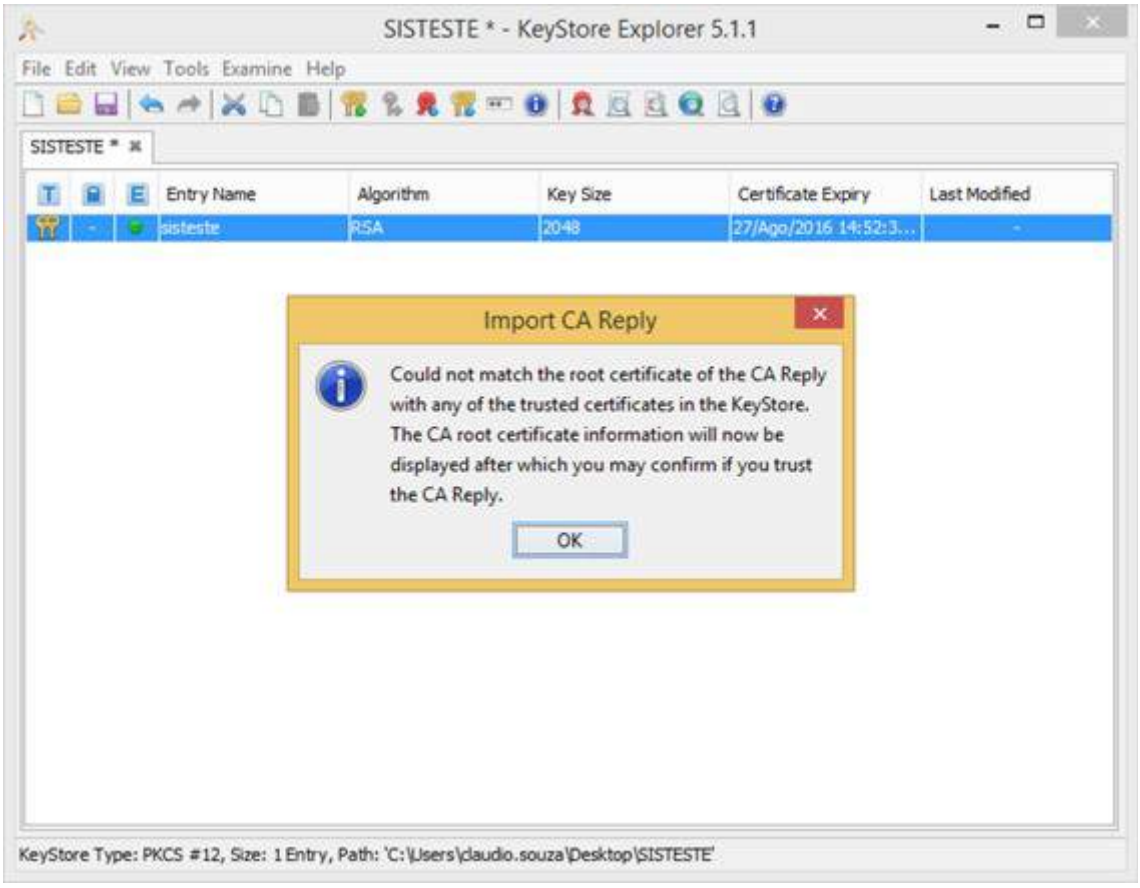
1.1 Abra o site disponível na seguinte URL: https://www.sslshopper.com/ssl-converter.html

1.2 Selecione o arquivo .p7b recebido da Autoridade de Registro, informe o tipo do arquivo **'P7B/PKCS#7'** e converter para **'Standard**

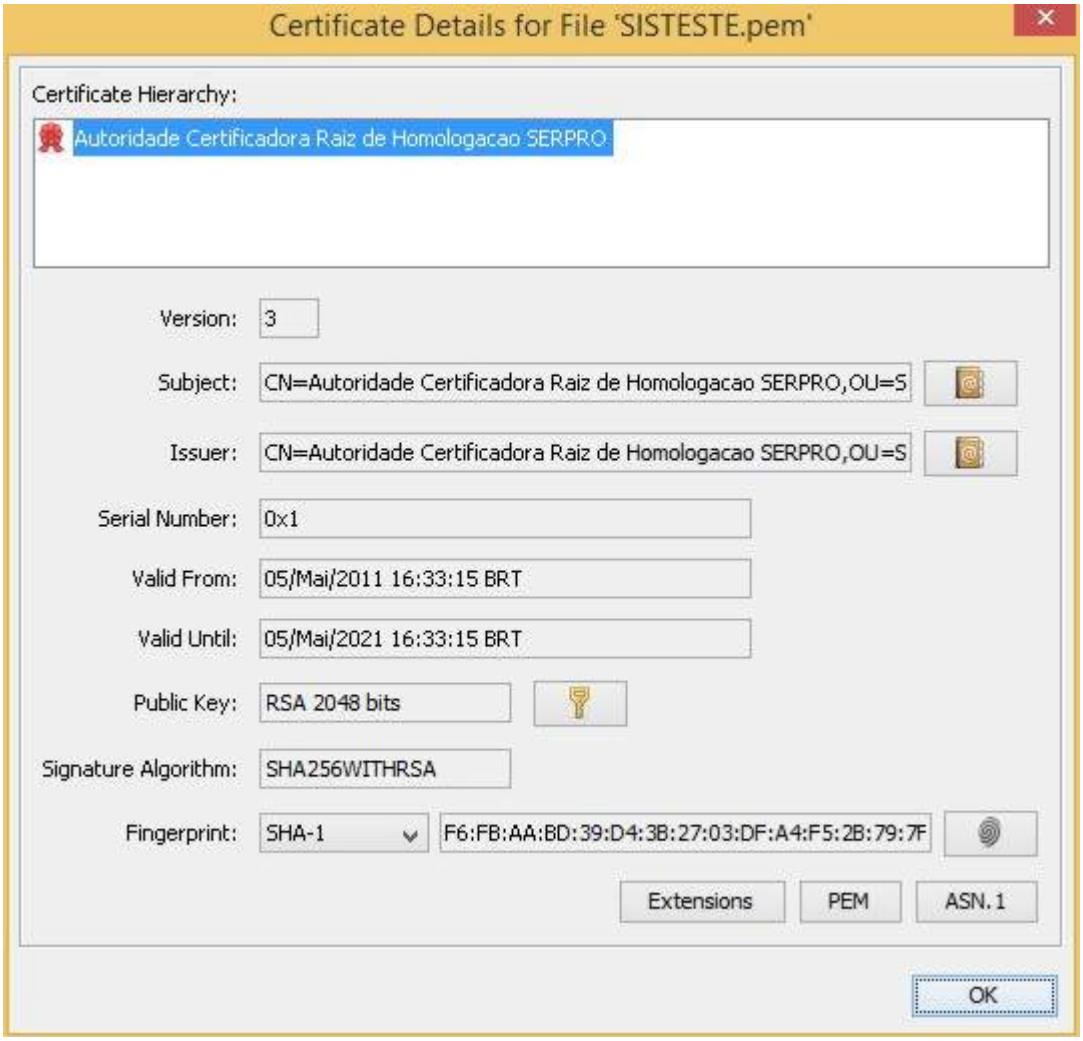
**PEM'** conforme exemplo abaixo:


2 No sistema KeyStore, utilize a opção **"Import CA Reply"** clicando com o botão direito sobre a opção "<sistema>.key" para importar a resposta da Autoridade de Registro. Selecione o arquivo convertido (*.PEM):

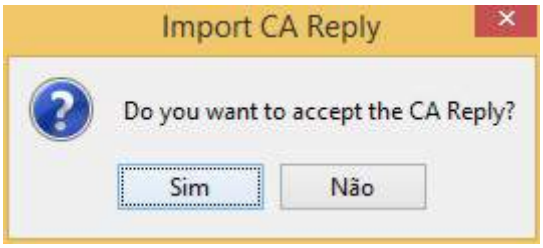

afnsisytem * - KeyStore Explorer 5.0.1
ile Edit View Tools Examine Help
afnsisytem *
Entry Name
Algorithm
afnsisystem.gov.br
RSA
View Details
Cut Ctrl+X
Copy Ctrl+C
Export
Generate CSR
Import CA Reply
Edit Certificate Chain
Sign
Unlock
Set Password
Delete
Rename


SISTESTE * - KeyStore Explorer 5.1.1
File Edit View Tools Examine Help
SISTESTE *
Entry Name
Algorithm
Key Size
Certificate Expiry
Last Modified
sisteste
RSA
2048
27/Ago/2016 14:52:3...
Import CA Reply
Could not match the root certificate of the CA Reply with any of the trusted certificates in the KeyStore. The CA root certificate information will now be displayed after which you may confirm if you trust the CA Reply.
OK
KeyStore Type: PKCS #12, Size: 1 Entry, Path: 'C:\Users\claudio.souza\Desktop\SISTESTE'

3 Ao apertar OK, aparecerá esta tela:

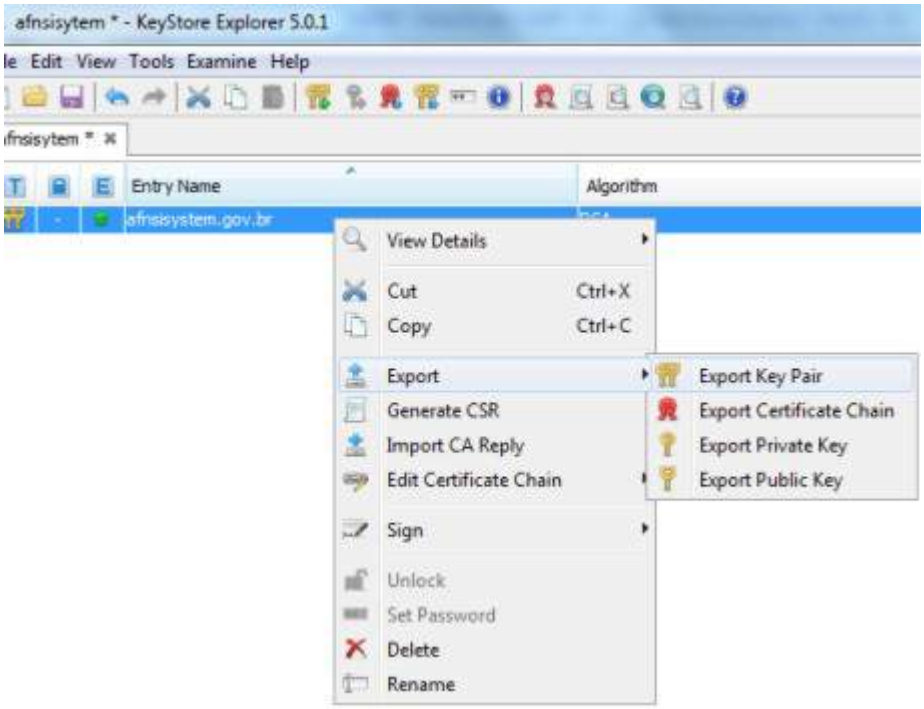



4 Ao apertar OK, aparecerá esta tela:

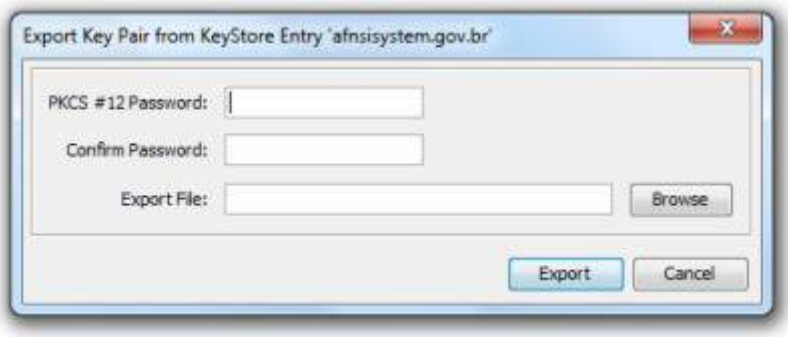



5 Selecione Sim.

6 Faça a exportação do par de chaves. Utilize a opção **"Export Key Pair"** clicando com o botão direito sobre a opção "sistema.key". A saída desta exportação será um arquivo (*.pfx):




7 Forneça uma senha para a sua chave privada:




8 Após gerado o arquivo (*.pfx), utilize-o para fazer a autenticação mútua entre SISDEPEN e o Sistema Externo:

# 12. ANEXO II - Como gerar um certificado de Homologação [Linux + OpenSSL]

## 12.1. Solicitar um certificado

1 Acessar o site: https://certificadoshom.serpro.gov.br/arserprossl/;

2 Navegar no seguinte fluxo: **'Meu Certificado -> Solicitar -> Equipamento'**;

2.1 Acionar o link **'Equipamento A1 (Institucional)'** caso o seu Órgão tenha contrato com o SERPRO para emissão de certificados;

2.2 Acionar o link **'Certificado de Equipamento A1 - R$ XXX,XX'** caso o seu Órgão não tenha contrato com o SERPRO para emissão de certificados;

3 Preencher o Formulário de Solicitação para Certificado Digital - Equipamento A1;

3.1 No campo **'* URL'** preencher com o DNS ou Nome da aplicação. O usuário não poderá usar o caractere barra "/" neste campo;

4 Após finalizada a solicitação o sistema irá exibir informações detalhadas dos procedimentos adicionais que deverão ser realizados para a emissão do Certificado Digital.

4.1 Envie um e-mail para o endereço certificados-homologacao-sisdepen@serpro.gov.br com o seguinte texto:

Solicito a geração de certificado digital para testes.

**Número de Referência do Pedido:** <numero>
**Tipo de Certificado:** Equipamento A1
**Ambiente da Solicitação:** https://certificadoshom.serpro.gov.br/arserprossl/
**Sistema:** <sistema>

4.1.1 <numero> é o número da solicitação obtido no *passo 4 deste tópico*.

4.1.2 <sistema> é o nome do sistema a ser integrado com o SISDEPEN informado no campo **'* URL'**;

## 12.2. Preparar o ambiente para geração do par de chaves

Observação: As instruções a seguir foram baseadas em um ambiente Linux utilizando OpenSSL e Keytool.

**Dica 1:** Realize todo o processo em uma mesma máquina/servidor.
**Dica 2:** Se você não tem familiaridade com este processo, crie uma senha única para informar sempre que for solicitado.
**Dica 3:** Crie senhas com caracteres especiais e números.

1 Localize em seu diretório de arquivos a pasta que cotenha o arquivo **'openssl.cnf'**.
- 1.1 Normalmente fica em: '/usr/lib/ssl' ou '/etc/ssl';
- 1.2 Se não estiver nesses locais, vá até o sistema de arquivos (pasta raiz) e pesquise por 'openssl.cnf' na lupa de pesquisa do sistema operacional.

2 Verifique nas propriedades do arquivo qual é a sua localização ou faça uma cópia deste arquivo para uma pasta de sua preferência.

## 12.3. Gerar requisição para Autoridade de Registro (.CSR)

1 Abra a linha de comando (shell) e navegue até a pasta onde está o arquivo 'openssl.cnf';

2 Ao chegar na pasta do arquivo 'openssl.cnf' digite o comando abaixo para gerar ao mesmo tempo a sua chave privada '<chave>.key' e o arquivo com a requisição a ser informada no momento da instalação do certificado no site da Autoridade de Registro 'requisicao.csr':
- 2.1 **openssl req -newkey rsa:2048 -keyout <chave>.key -keyform PEM -SHA256 -out requisicao.csr -config openssl.cnf**
- 2.2 substitua '<chave>' por um nome desejado para a sua chave privada, de preferência o nome do sistema que consumirá os serviços do Novo SISDEPEN;

3 O terminal solicitará uma senha para acesso à sua chave pridada;

3.1 'Enter PEM pass phrase:' e 'Verifying - Enter PEM pass phrase:'. Preencha com uma senha e guarde-a pois será utilizada futuramente.

4 O terminal solicitará que você insira uma série de informações que serão incorporadas em sua solicitação de certificado. A **única** informação necessária para a Autoridade de Registro do SERPRO é o campo **'Common Name'** que deverá ser preenchido com a mesma informação adicionada no campo **'* URL'** do Formulário de Solicitação para Certificado Digital - Equipamento A1 (Institucional) [ *Passo 3 do tópico Solicitar um Certificado*].

4.1 Para as demais perguntas basta teclar <ENTER> sem informar nenhuma informação que o site da Autoridade de Registro completará com as informações atualizadas retiradas do Formulário de Solicitação para Certificado Digital;

5 Após a execução do *passo 4 deste tópico* serão gerados dois arquivos na mesma pasta que está armazenado o arquivo 'openssl.cnf':

5.1 <chave>.key - sua chave privada.

5.2 requisicao.csr - arquivo com o conteúdo a ser informado no site da Autoridade de Registro no momento da instalação;

6 Aguarde o e-mail da Autoridade de Registro informando que o seu certificado está aprovado.

## 12.4. Instalar um certificado

1 Uma vez que a solicitação de certificado já foi aprovada por uma Autoridade de Registro (A Autoridade de Registro envia um e-mail informando a aprovação), o último passo para a obtenção do Certificado Digital é a instalação.

2 Acessar o site: https://certificadoshom.serpro.gov.br/arserprossl/;

3 Acessar o menu **"Meu Certificado → Baixar"**

3.1 Neste ponto o solicitante deverá apresentar suas credenciais de acesso e em seguida será apresentada a tela para instalação/download do seu Certificado Digital.

4 Na tela de instalação do certificado, informar no único campo texto da tela o conteúdo do arquivo gerado no *passo 5.2 do tópico Gerar requisição*

*para Autoridade de Registro (.CSR)* e acione o botão 'Salvar Certificado';

5 O site disponibilizará um arquivo com o nome do URL informada e extensão .p7b **'<sistema>.p7b'**. Este arquivo contém a sua chave pública assinada e a cadeia confiável da Autoridade de Registro;

5.1 Salve-o na mesma pasta do arquivo 'openssl.cnf'

## 12.5. Preparação e Montagem do certificado digital para utilização pela aplicação cliente

1 Abra a linha de comando (shell) e navegue até a pasta onde está o arquivo 'openssl.cnf';

2 Ao chegar na pasta do arquivo 'openssl.cnf' digite os comandos abaixo nesta respectiva ordem:

2.1 **openssl pkcs7 -print_certs -in <sistema>.p7b -out <sistema>.cer** (Converte o arquivo .p7b para um arquivo de chaves concatenadas);

2.2 **openssl pkcs12 -export -in <sistema>.cer -inkey <chave>.key -out <sistema>.pfx** (Exporta em um arquivo único a sua chave privada, a chave pública e a cadeia da Autoridade de Registro. Esse arquivo será importante para teste do cadastro no Novo SISDEPEN);

2.3 **keytool -importkeystore -srckeystore <sistema>.pfx -destkeystore <sistema>.keystore -deststoretype JKS -srcstoretype PKCS12** (Cria uma keystore e importa todas as chaves e cadeias criadas neste roteiro para dentro da keystore. Esse arquivo é utilizado por muitas aplicações clientes);

3 Ao final deste processo, na pasta onde está o arquivo 'openssl.cnf', teremos os seguintes arquivos:

3.1 openssl.cnf

3.2 requisicao.csr

3.3 <sistema>.p7b

3.4 <sistema>.cer

3.5 <sistema>.pfx

3.6 <sistema>.keystore

# 13. ANEXO III - Como gerar um certificado de Produção [Windows + Keystore explorer 5.0.1]

## 13.1. Solicitar um certificado

1 Acessar o site: https://certificados.serpro.gov.br/arserprossl/;

2 Navegar no seguinte fluxo: **'Meu Certificado -> Solicitar -> Equipamento'**;

**2.1** Acionar o link **'Equipamento A1 (Institucional)'** caso o seu Órgão tenha contrato com o SERPRO para emissão de certificados;

**2.2** Acionar o link **'Certificado de Equipamento A1 - R$ XXX,XX'** caso o seu Órgão não tenha contrato com o SERPRO para emissão de certificados;

3 Preencher o Formulário de Solicitação para Certificado Digital - Equipamento A1;

**3.1** No campo **'* URL'** preencher com o DNS ou Nome da aplicação. O usuário não poderá usar o caractere barra "/" neste campo;

4 Após finalizada a solicitação o sistema irá exibir informações detalhadas dos procedimentos adicionais que deverão ser realizados para a emissão do Certificado Digital.

**4.1** Para a emissão do certificado de produção será necessária a apresentação presencial pelo representante legal do certificado dos documentos originais informados no Formulário de Solicitação para Certificado Digital;

**4.1.1** Os Documentos Necessários estão descritos no link: https://certificados.serpro.gov.br/arserprossl/ **'Informações -> Documentos Necessários'**;

**4.1.2** Os endereços dos Postos de Atendimento estão disponíveis em: https://certificados.serpro.gov.br/arserprossl/ **'Informações -> Endereço de Posto de Atendimento'**;

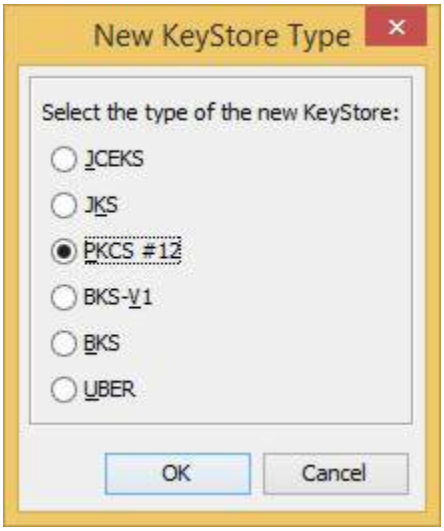
## 13.2. Preparar o ambiente para geração do par de chaves

Observação: As instruções a seguir foram baseadas em um ambiente Windows com o programa Keystore Explore 5.0.1

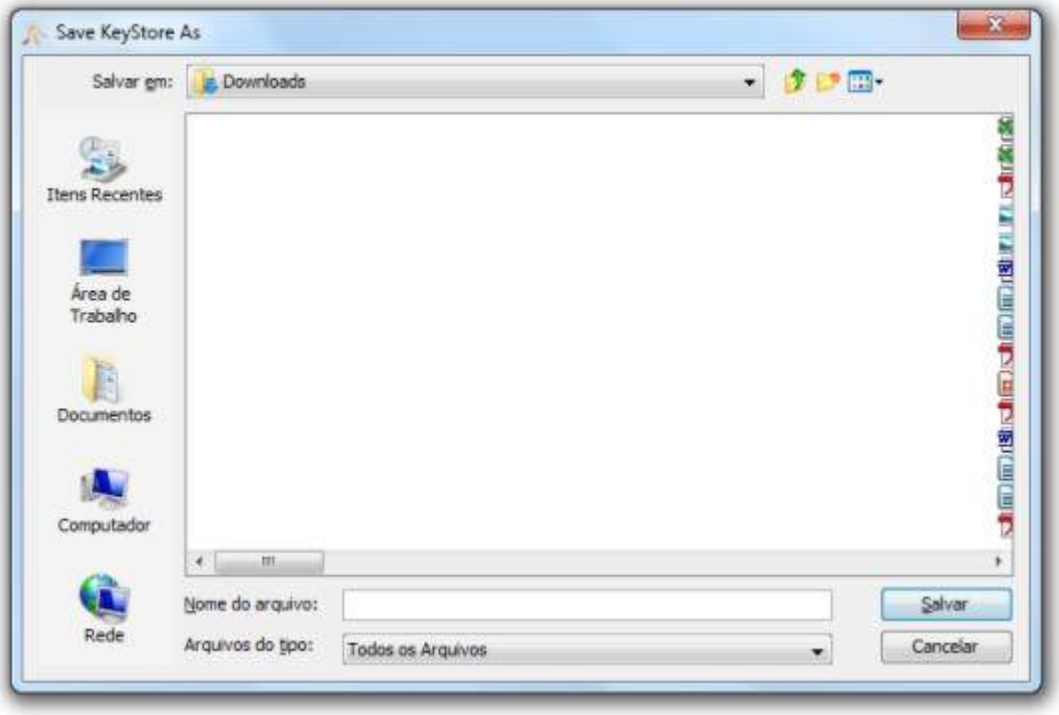
**Dica 1:** Realize todo o processo em uma mesma máquina/servidor.
**Dica 2:** Se você não tem familiaridade com este processo, crie uma senha única para informar sempre que for solicitado.
**Dica 3:** Crie senhas com caracteres especiais e números.

1 Faça o download do keyStore Explorer em http://keystore-explorer.sourceforge.net/downloads.php;

2 Abra o KeyStore Explorer e selecione a opção **"Create a new KeyStore"**:

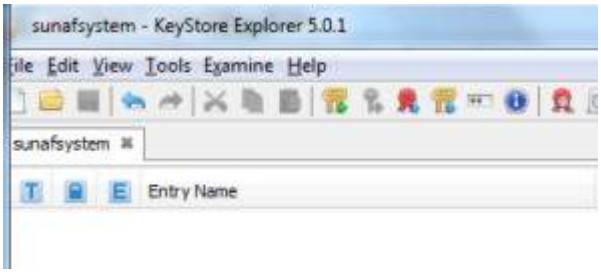



3 Salve a keystore com o nome do seu sistema:




4 O programa irá te solicitar uma senha para este keystore:

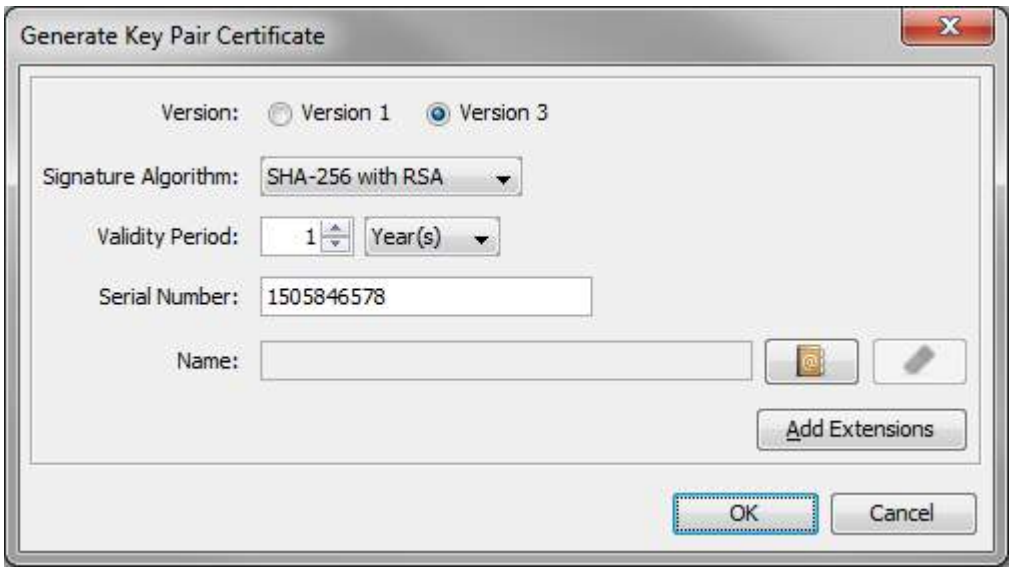

5 Observe que o Keystore (Nome da Aba) foi criado com o nome informado:




6 Acione o botão de geração do par de chaves:

7 Informe o algoritmo 'RSA' e o tamanho da chave '2.048':

8 Informe a **versão 3**, o algoritmo de assinatura **'SHA-256 with RSA'**, 1 ano de validade:

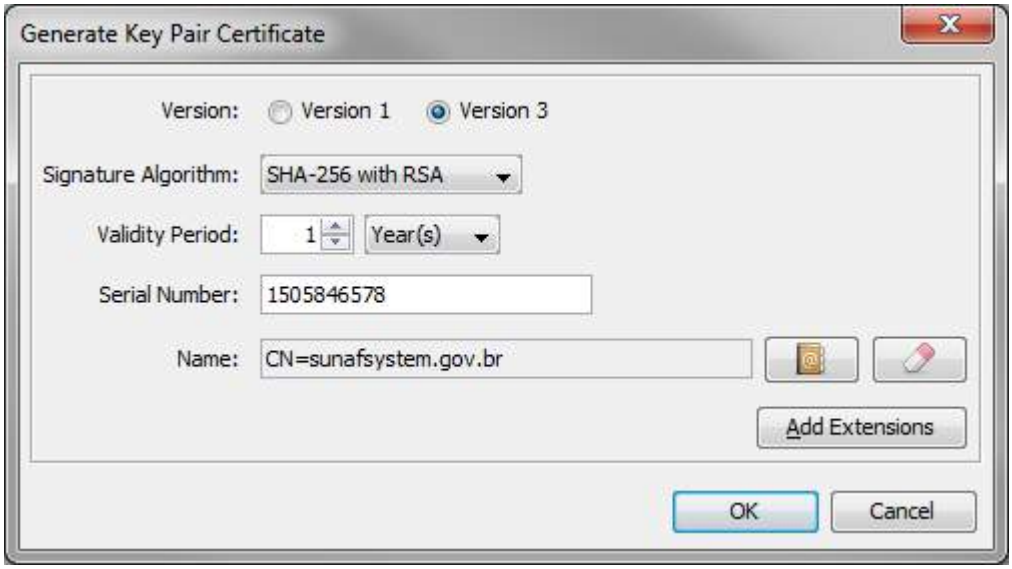



9 Edite o Nome do certificado acionando o botão 'Edit name':


10 A **única** informação necessária para a Autoridade de Registro do SERPRO é o campo **'Common Name (CN):'** que deverá ser preenchido com a mesma informação adicionada no campo **'* URL'** do Formulário de Solicitação para Certificado Digital - Equipamento A1. Os demais campos deixar em branco:

**Obs: o usuário não poderá usar o caractere barra "/" no CN**


11 Selecione **'OK'** e verifique que no campo **'Name'** terá apenas a informação 'CN=<sistema>':

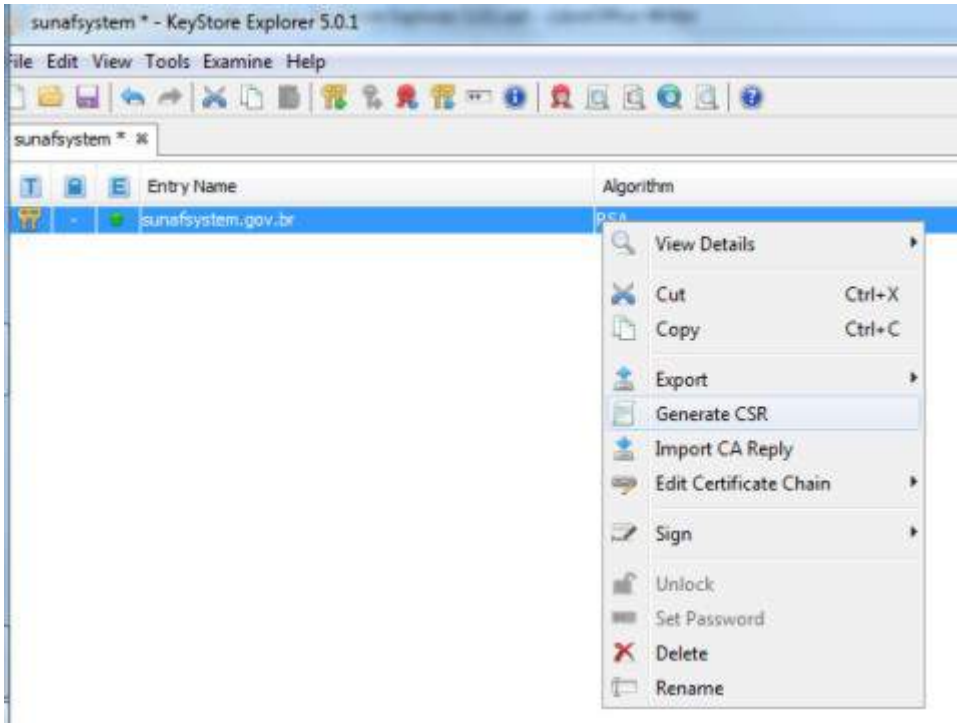



12 Selecione 'OK' e o sistema irá solicitar um alias para o par de chaves a ser gerado. Informe a mesma informação adicionada no campo **'* URL'** do Formulário de Solicitação para Certificado Digital - Equipamento A1:


13 Confirme e o sistema exibirá uma mensagem de sucesso na geração do par de chaves:


## 13.3. Gerar requisição para Autoridade de Registro (.CSR)

1 Clique com o botão direito sobre a keystore e acione a opção 'Generate CSR' para gerar a requisição a ser informada no momento da instalação do certificado no site da Autoridade de Registro **'requisicao.csr'**:



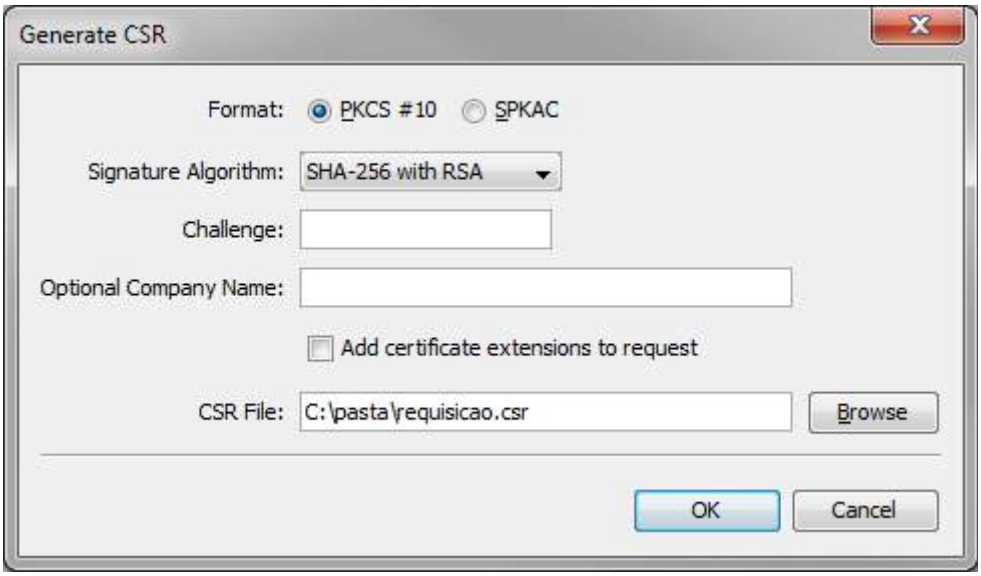

2 Informe como parâmetros para o arquivo CSR os seguintes valores:

2.1 Format: **PKCS #10**;

2.2 Signature Algorithm: **SHA-256 with RSA**;

2.3 Challenge: **(Deixe em branco)**;

2.4 CSR File: **'requisicao.csr'**



3 Após a execução do *passo 2 deste tópico* será gerado o arquivo **'requisicao.csr'** com o conteúdo a ser informado no site da Autoridade de Registro no momento da instalação;


4 Aguarde o e-mail da Autoridade de Registro informando que o seu certificado está aprovado.

## 13.4. Instalar um certificado

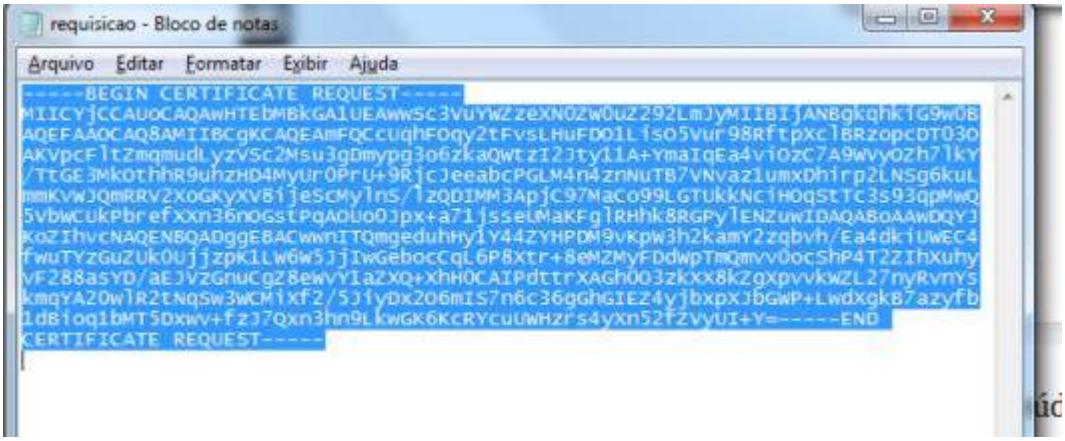
1 Uma vez que a solicitação de certificado já foi aprovada por uma Autoridade de Registro (A Autoridade de Registro envia um e-mail informando a aprovação), o último passo para a obtenção do Certificado Digital é a instalação.

2 Acessar o site: https://certificados.serpro.gov.br/arserprossl/;

3 Acessar o menu **"Meu Certificado → Baixar"**

3.1 Neste ponto o solicitante deverá apresentar suas credenciais de acesso e em seguida será apresentada a tela para instalação/download do seu Certificado Digital.

4 Na tela de instalação do certificado, informar no único campo texto da tela o conteúdo do arquivo gerado no *passo 2.4 do tópico Gerar requisição para Autoridade de Registro (.CSR)* e acione o botão **'Salvar Certificado'**;




5 O site disponibilizará um arquivo com o nome do URL informada e extensão .p7b **'<sistema>.p7b'**. Este arquivo contém a sua chave pública assinada e a cadeia confiável da Autoridade de Registro. Salve-o em seu computador e por segurança faça uma cópia de backup.

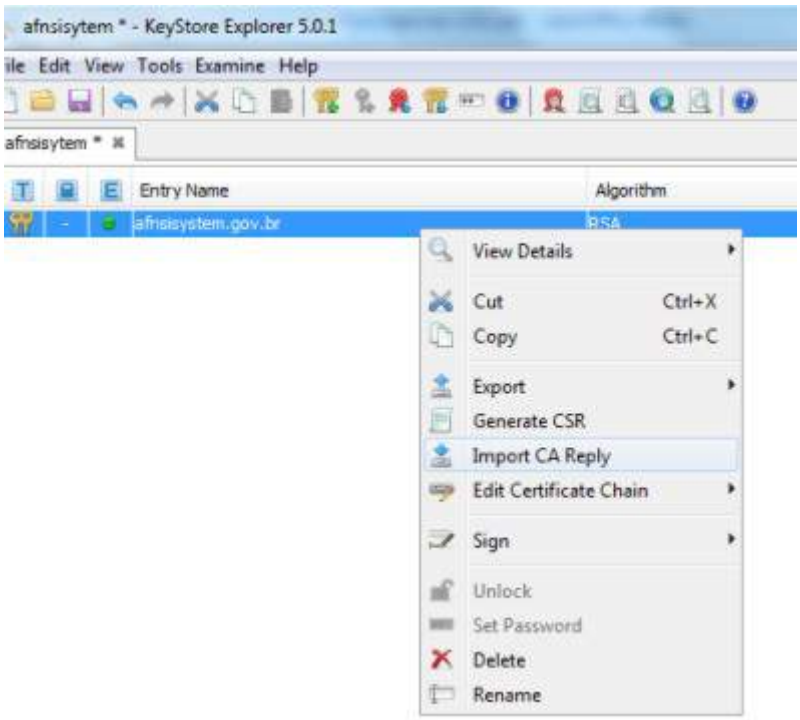
## 13.5. Preparação e Montagem do certificado digital para utilização pela aplicação cliente

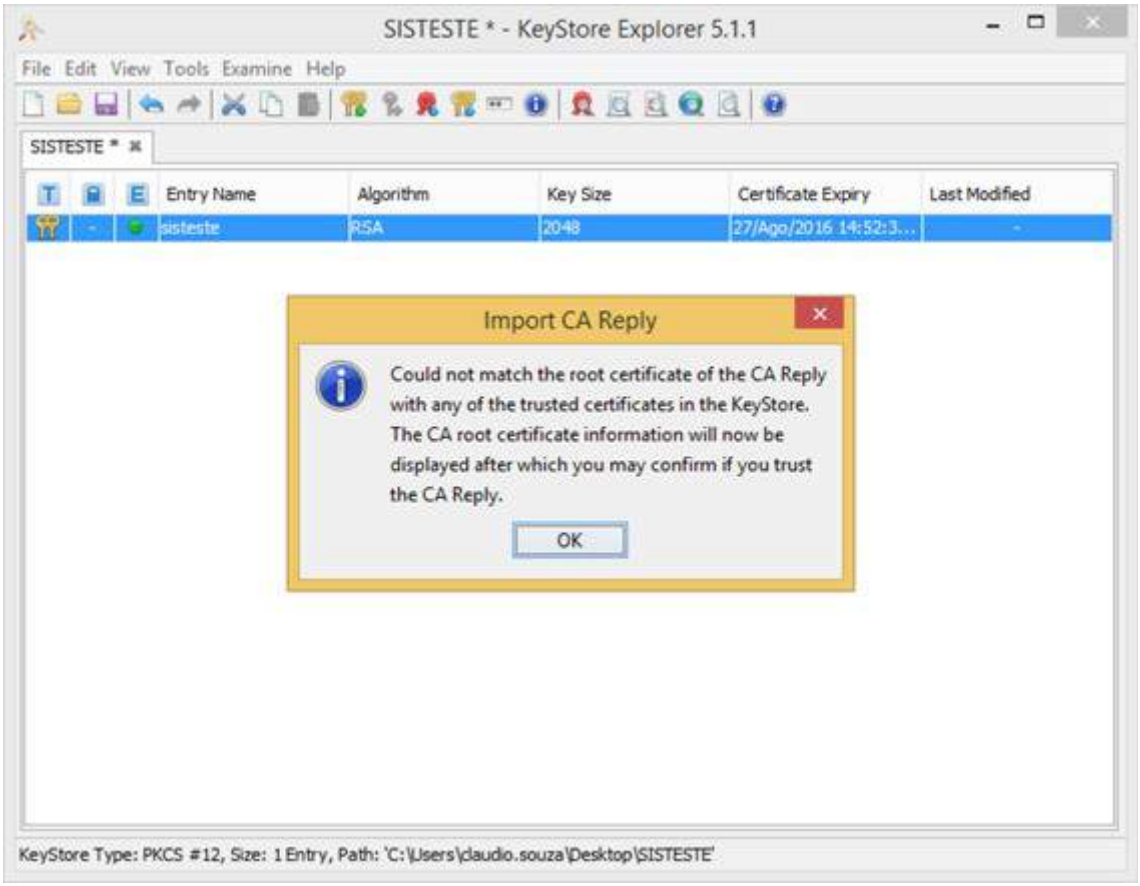
1 Converta o arquivo .p7b para o formato PEM que é reconhecido pelo KeyStore Explorer.

2 Abra o site disponível na seguinte URL: https://www.sslshopper.com/ssl-converter.html

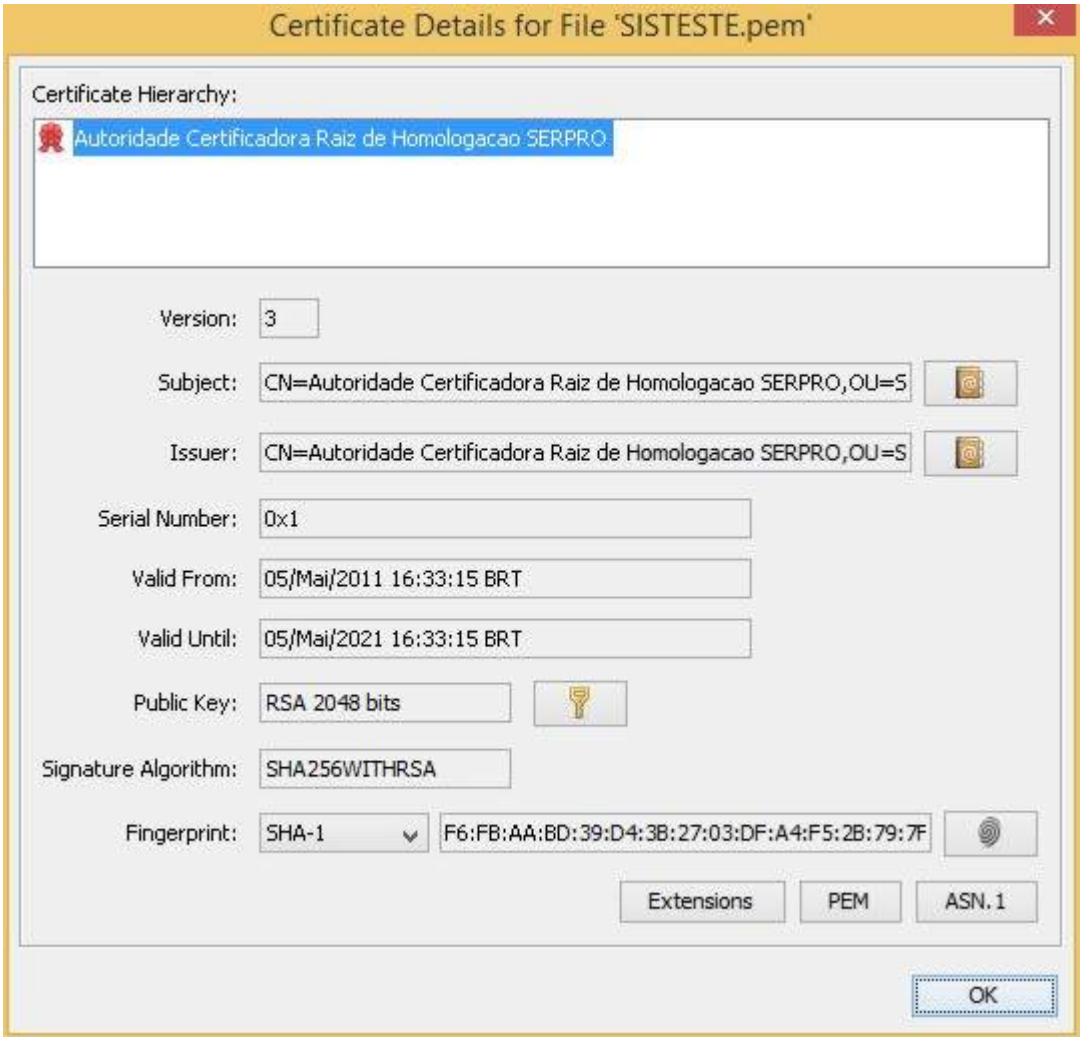
3 Selecione o arquivo .p7b recebido da Autoridade de Registro, informe o tipo do arquivo **'P7B/PKCS#7'** e converter para **'Standard PEM'** conforme exemplo abaixo:


4 No sistema KeyStore, utilize a opção **"Import CA Reply"** clicando com o botão direito sobre a opção "<sistema>.key" para importar a resposta da Autoridade de Registro. Selecione o arquivo convertido (*.PEM)

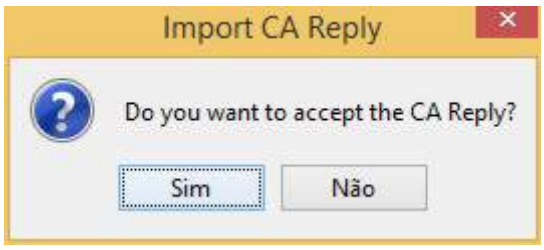





5 Ao apertar OK, aparecerá esta tela:



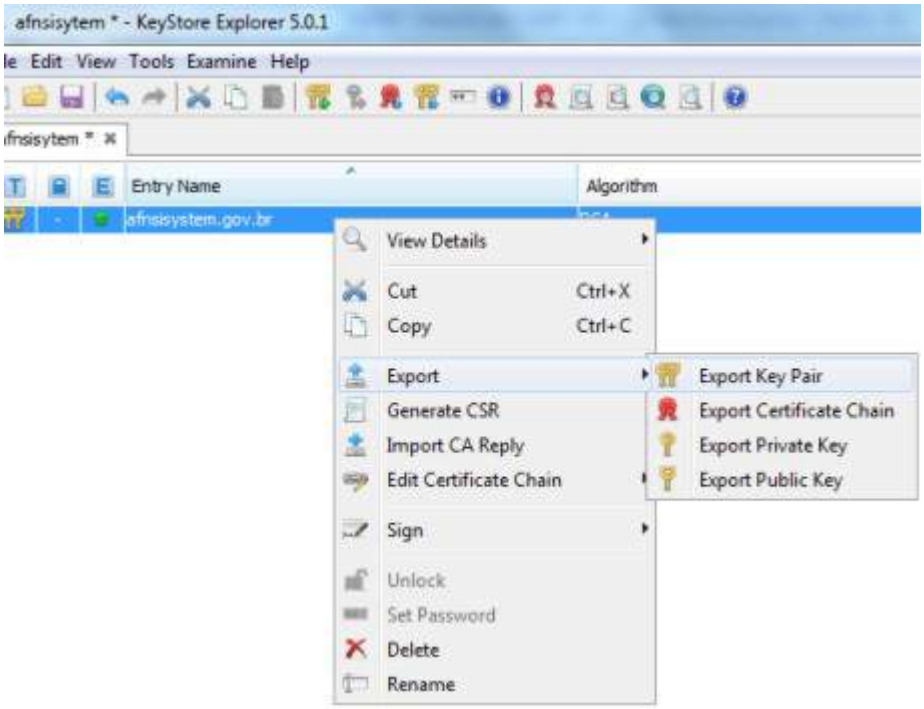

6 Ao apertar OK, aparecerá esta tela:



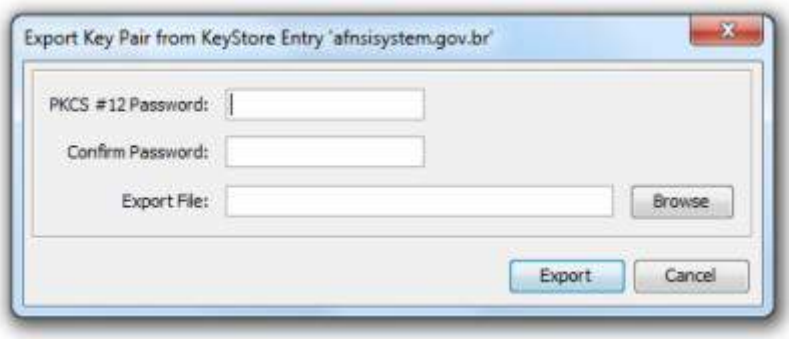

7 Tecle Sim.

8 Faça a exportação do par de chaves.

9 Utilize a opção **"Export Key Pair"** clicando com o botão direito sobre a opção "sistema.key". A saída desta exportação será um arquivo (*.pfx):




10 Forneça uma senha para a sua chave privada:




11 Após gerado o arquivo (*.pfx), utilize-o para fazer a autenticação mútua entre SISDEPEN e o Sistema Externo.

# 14. ANEXO IV - Como gerar um certificado de Produção [Linux + OpenSSL]

## 14.1. Solicitar um certificado

1 Acessar o site: https://certificados.serpro.gov.br/arserprossl/;

2 Navegar no seguinte fluxo: **'Meu Certificado -> Solicitar -> Equipamento'**;

2.1 Acionar o link **'Equipamento A1 (Institucional)'** caso o seu Órgão tenha contrato com o SERPRO para emissão de certificados;

2.2 Acionar o link **'Certificado de Equipamento A1 - R$ XXX,XX'** caso o seu Órgão não tenha contrato com o SERPRO para emissão de certificados;

3 Preencher o Formulário de Solicitação para Certificado Digital - Equipamento A1;

3.1 No campo **'* URL'** preencher com o DNS ou Nome da aplicação. O usuário não poderá usar o caractere barra "/" neste campo;

4 Após finalizada a solicitação o sistema irá exibir informações detalhadas dos procedimentos adicionais que deverão ser realizados para a emissão do Certificado Digital.

4.1 Para a emissão do certificado de produção será necessária a apresentação presencial pelo representante legal do certificado dos documentos originais informados no Formulário de Solicitação para Certificado Digital;

4.1.1 Os Documentos Necessários estão descritos no link: https://certificados.serpro.gov.br/arserprossl/ **'Informações -> Documentos Necessários'**;

4.1.2 Os endereços dos Postos de Atendimento estão disponíveis em: https://certificados.serpro.gov.br/arserprossl/ **'Informações -> Endereço de Posto de Atendimento'**;

## 14.2. Preparar o ambiente para geração do par de chaves

Observação: As instruções a seguir foram baseadas em um ambiente Linux utilizando OpenSSL e Keytool.

**Dica 1:** Realize todo o processo em uma mesma máquina/servidor.
**Dica 2**: Se você não tem familiaridade com este processo, crie uma senha única para informar sempre que for solicitado.
**Dica 3:** Crie senhas com caracteres especiais e números.

1 Localize em seu diretório de arquivos a pasta que cotenha o arquivo **'openssl.cnf'**.
- 1.1 Normalmente fica em: '/usr/lib/ssl' ou '/etc/ssl';
- 1.2 Se não estiver nesses locais, vá até o sistema de arquivos (pasta raiz) e pesquise por 'openssl.cnf' na lupa de pesquisa do sistema operacional.

2 Verifique nas propriedades do arquivo qual é a sua localização ou faça uma cópia deste arquivo para uma pasta de sua preferência.

## 14.3. Gerar requisição para Autoridade de Registro (.CSR)

1 Abra a linha de comando (shell) e navegue até a pasta onde está o arquivo 'openssl.cnf';

2 Ao chegar na pasta do arquivo 'openssl.cnf' digite o comando abaixo para gerar ao mesmo tempo a sua chave privada '<chave>.key' e o arquivo com a requisição a ser informada no momento da instalação do certificado no site da Autoridade de Registro 'requisicao.csr':
- 2.1 **openssl req -newkey rsa:2048 -keyout <chave>.key -keyform PEM -SHA256 -out requisicao.csr -config openssl.cnf**
- 2.2 substitua '<chave>' por um nome desejado para a sua chave privada, de preferência o nome do sistema que consumirá os serviços do Novo SISDEPEN;

3 O terminal solicitará uma senha para acesso à sua chave pridada;

3.1 'Enter PEM pass phrase:' e 'Verifying - Enter PEM pass phrase:'. Preencha com uma senha e guarde-a pois será utilizada futuramente.

4 O terminal solicitará que você insira uma série de informações que serão incorporadas em sua solicitação de certificado. A **única** informação necessária para a Autoridade de Registro do SERPRO é o campo **'Common Name'** que deverá ser preenchido com a mesma informação adicionada no campo **'* URL'** do Formulário de Solicitação para Certificado Digital - Equipamento A1 (Institucional) [ *Passo 3 do tópico Solicitar um certificado*].

4.1 Para as demais perguntas basta teclar <ENTER> sem informar nenhuma informação que o site da Autoridade de Registro completará com as informações atualizadas retiradas do Formulário de Solicitação para Certificado Digital;

5 Após a execução do *passo 4 deste tópico* serão gerados dois arquivos na mesma pasta que está armazenado o arquivo 'openssl.cnf':

5.1 <chave>.key - sua chave privada.

5.2 requisicao.csr - arquivo com o conteúdo a ser informado no site da Autoridade de Registro no momento da instalação;

6 Aguarde o e-mail da Autoridade de Registro informando que o seu certificado está aprovado.

## 14.4. Instalar um certificado

1 Uma vez que a solicitação de certificado já foi aprovada por uma Autoridade de Registro (A Autoridade de Registro envia um e-mail informando a aprovação), o último passo para a obtenção do Certificado Digital é a instalação.

2 Acessar o site: https://certificados.serpro.gov.br/arserprossl/;

3 Acessar o menu "**Meu Certificado → Baixar**"

3.1 Neste ponto o solicitante deverá apresentar suas credenciais de acesso e em seguida será apresentada a tela para instalação/download do seu Certificado Digital.

4 Na tela de instalação do certificado, informar no único campo texto da tela o conteúdo do arquivo gerado no *passo 5.2 do tópico Gerar requisição*

*para Autoridade de Registro (.CSR)* e acione o botão 'Salvar Certificado';

5 O site disponibilizará um arquivo com o nome do URL informada e extensão .p7b **'<sistema>.p7b'**. Este arquivo contém a sua chave pública assinada e a cadeia confiável da Autoridade de Registro;

6 Salve-o na mesma pasta do arquivo 'openssl.cnf';

## 14.5. Preparação e Montagem do certificado digital para utilização pela aplicação cliente

1 Abra a linha de comando (shell) e navegue até a pasta onde está o arquivo 'openssl.cnf';

2 Ao chegar na pasta do arquivo 'openssl.cnf' digite os comandos abaixo nesta respectiva ordem:

2.1 **openssl pkcs7 -print_certs -in <sistema>.p7b -out <sistema>.cer** (Converte o arquivo .p7b para um arquivo de chaves concatenadas);

2.2 **openssl pkcs12 -export -in <sistema>.cer -inkey <chave>.key -out <sistema>.pfx** (Exporta em um arquivo único a sua chave privada, a chave pública e a cadeia da Autoridade de Registro. Esse arquivo será importante para teste do cadastro no Novo SISDEPEN);

2.3 **keytool -importkeystore -srckeystore <sistema>.pfx -destkeystore <sistema>.keystore -deststoretype JKS -srcstoretype PKCS12** (Cria uma keystore e importa todas as chaves e cadeias criadas neste roteiro para dentro da keystore. Esse arquivo é utilizado por muitas aplicações clientes);

3 Ao final deste processo, na pasta onde está o arquivo 'openssl.cnf', teremos os seguintes arquivos:

3.1 openssl.cnf

3.2 requisicao.csr

3.3 <sistema>.p7b

3.4 <sistema>.cer

3.5 <sistema>.pfx

3.6 <sistema>.keystore