

Manual de Instalação - Agente CliSiTef

Manual de Instalação

Versão 1.03

Esclarecimentos

- O usuário deste documento é o responsável por garantir que está de posse da versão mais atualizada.
- Qualquer usuário pode utilizar essa cópia para sugerir alterações no documento.
- Todos os pedidos de alteração devem ser direcionados ao responsável pelo documento (ver coluna “Autor” do item “Histórico de Alterações” neste documento).
- Somente o responsável consolida os pedidos de alteração.
- Somente o responsável pode alterar o número da versão deste documento.
- A versão deste documento é composta por dois números, separados por um ponto. O número à esquerda do ponto é incrementado sempre que a alteração feita determine alguma mudança no Software (ou no conjunto de Software). O número à direita, por sua vez, é incrementado quando a alteração feita não determina mudanças no Software (ex.: detalhar alguma funcionalidade que já exista; efetuar correções, etc). O número da direita é zerado toda vez que o número da esquerda for incrementado. Os números à esquerda e direita do ponto podem crescer conforme a necessidade, porém sem utilizar zeros à esquerda.

Sumário

1	Introdução	4
2	Objetivo.....	4
3	Público-Alvo.....	4
4	Criando um pacote <i>master</i> para instalação em estações de trabalho	5
4.1	Pré-requisitos:	5
4.2	Instalação do <i>OpenSSL</i>	5
4.3	Conteúdo do pacote AgenteCliSiTef:	7
4.4	Gerando os arquivos de Certificado.....	8
4.5	Instalando o AgenteCliSiTef como um serviço do Windows.....	12
4.6	Criando um pacote <i>master</i> para instalação em estações de trabalho	13
5	Instalação em estações de trabalho com pacote <i>master</i>	14
6	Gerenciamento dos Certificados	14
7	Histórico de Alterações.....	15

1 Introdução

O *AgenteCliSiTef* é uma solução facilitadora para integração com a biblioteca *CliSiTef* no envio de transações ao concentrador de transações *SiTef*.



Para entendimento da solução *AgenteCliSiTef* consultar o documento “*AgenteCliSiTef - Especificação Técnica.pdf*”.

2 Objetivo

O objetivo deste documento é descrever os passos para instalação do *AgenteCliSiTef*.

3 Público-Alvo

Usuários do *AgenteCliSiTef* e Suporte da Software Express.

4 Criando um pacote *master* para instalação em estações de trabalho

4.1 Pré-requisitos:

- Windows 32
- *OpenSSL*

4.2 Instalação do *OpenSSL*

Para gerar os certificados e chaves de segurança e demais arquivos é necessário ter instalado na máquina o software *OpenSSL*.

Consulte na internet as opções para Download. Uma sugestão de download está disponível no link: <http://gnuwin32.sourceforge.net/packages/openssl.htm>. Selecione para download a opção "Complete package, except sources"

Homepage
<http://www.openssl.org>
Sources: <http://www.openssl.org/source>

Download

Description	Download	Size	Last change	Md5sum
• Complete package, except sources	Setup	4658384	4 December 2008	9d9e1c90bb4976a554f604e9e69ac0a0
• Sources	Setup	5348830	4 December 2008	d53a2219527bace9be1702b16cc4b64a
• Binaries	Zip	5906403	4 December 2008	a1d4868d6115b654f86c68821f6be8b0
• Developer files	Zip	1287741	4 September 2008	ed559e85a28e354672f304f4e667ffe3
• Documentation	Zip	2696271	23 August 2008	96eb1648cf73c3a22bf8f5a7694df186
• Sources	Zip	14375398	23 August 2008	7238e1e11ab2076e5ec13a23ba03c08e
• Original source	http://www.openssl.org/source/openssl-0.9.8h.tar.gz			

You can also download the files from the GnuWin32 [files page](#). New releases of the port of this package can be [monitored](#).

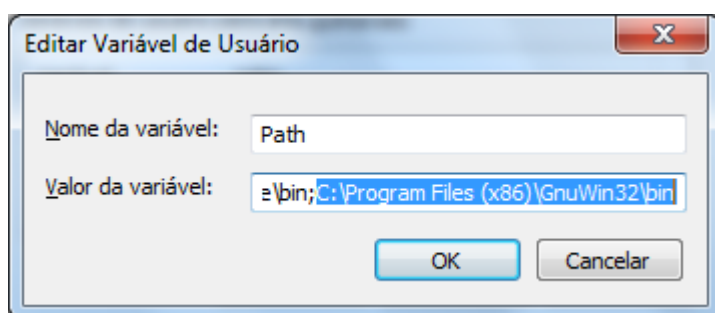
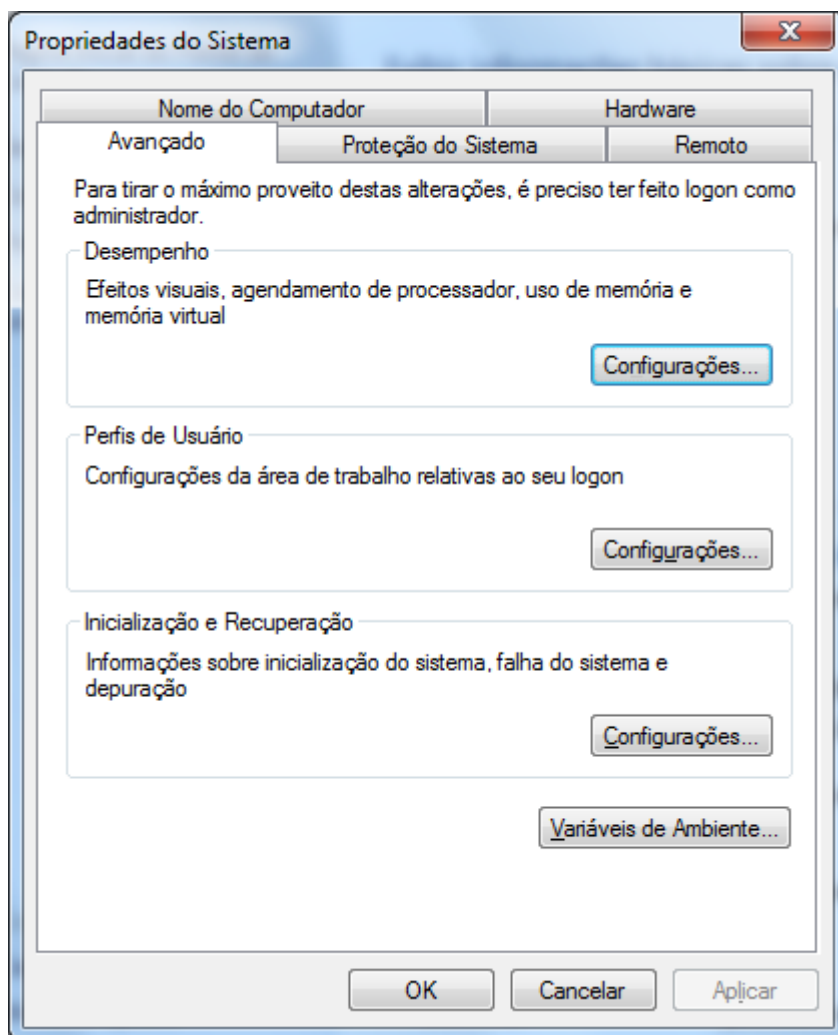
Installation, Usage and Help
[General Installation Instructions](#)
[GnuWin32 Help \(feature requests, bugs, etc\)](#)

Requirements

- Win32, i.e. MS-Windows 95 / 98 / ME / NT / 2000 / XP / 2003 / Vista / 2008 with msvcr.dll and msvcrt60.dll. If msvcr.dll or msvcrt60.dll is not in your Windows/System folder, get them from [Microsoft](#), or (msvcr.dll only) by installing [Internet Explorer](#) 4.0 or higher.





Configure a variável de ambiente do Windows "Path" para apontar o caminho onde está instalado o *openssl.exe* no seu computador.

Acesse as propriedades do Sistema, selecione "Variáveis de Ambiente" e adicione em Path o caminho de acordo com a instalação do seu computador.



4.3 Conteúdo do pacote AgenteCliSiTef:

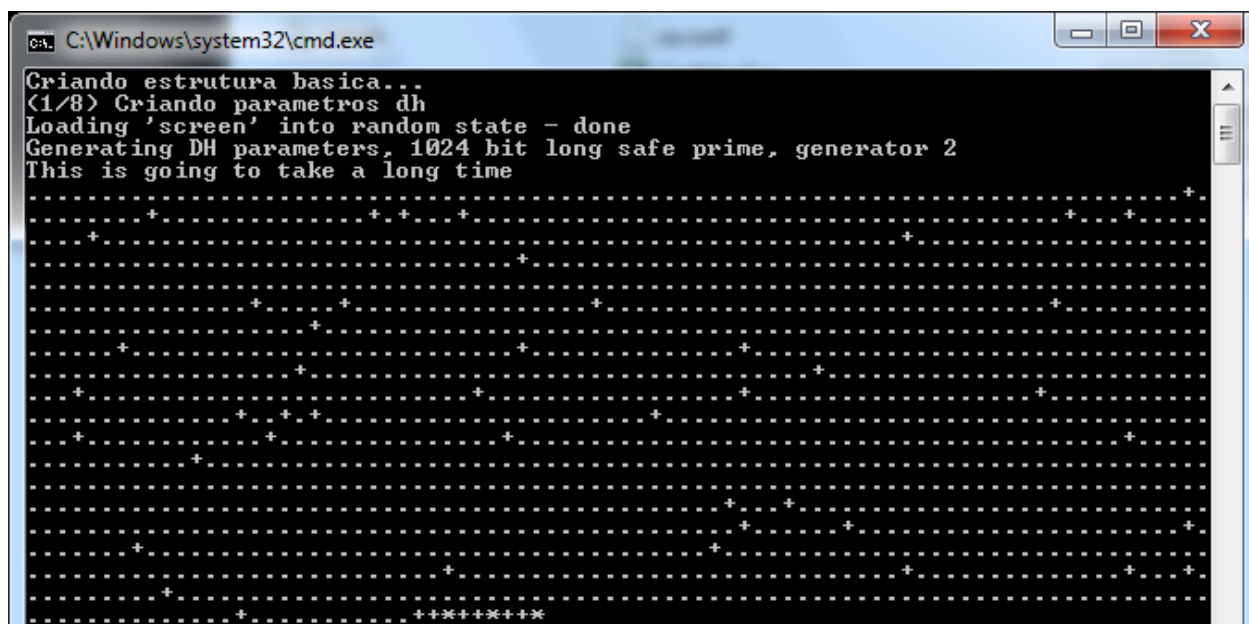
O pacote é composto pela seguinte estrutura de pastas e arquivos:

 bin	<ul style="list-style-type: none"> • <u>AgenteCliSiTef.exe</u> (Executável do <i>AgenteCliSiTef</i>) • <u>agenteclisitef.ini</u> (Configurador do <i>AgenteCliSiTef</i>) • <u>CliSiTef321.dll</u> (DLL de interface com o <i>SiTef</i>) • <u>CliSiTef.ini</u> (Arquivo de configuração da <i>CliSiTef</i>)
 helper	<ul style="list-style-type: none"> • <u>ca.conf</u> (arquivo de configuração para geração do certificado) • <u>CertMgr.Exe</u> (utilitário para instalação do Certificado no Windows) • <u>gera_certificados.bat</u> (utilitário para geração do certificado) • <u>gera_pacoteMaster.bat</u> (utilitário para geração do pacote master) • <u>instala.bat.pacoteMaster.txt</u> (fará parte do pacote master, é o utilitário para instalação do certificado da CA e do <i>AgenteCliSiTef</i> a partir do pacote master) • <u>localhost.conf</u> (arquivo de configuração para geração do certificado)
 html	Conjunto de páginas de Exemplo para integração com <i>AgenteClisitef</i> : <ul style="list-style-type: none"> ○ agenteCliSiTef.js ○ index.html ○ jquery-3.2.1.min.js ○ sessao.html ○ style.css ○ venda_com_sessao.html
 logs	<<vazia>>

4.4 Gerando os arquivos de Certificado

Execute o utilitário “gera_certificados.bat” (Este utilitário irá gerar os certificados e a chave privada que serão utilizados para validar as conexões SSL entre a Automação Web e o *AgenteCliSiTef*). Execute como Administrador (clique com o botão direito e escolha opção “Executar como Administrador”).

Passo 1/8 : Criando parâmetros dh



Passo 2/8 : Criando CA (Certificate Authority)

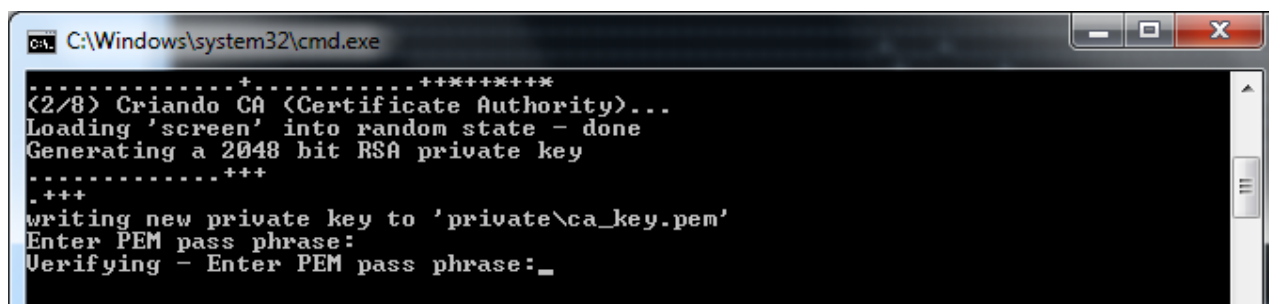
Será solicitado através do *prompt* a chave privada que será utilizada para gerar os certificados.



Ao informar a chave privada nos prompts “Enter PEM pass frase” e “Verifying – Enter PEM PASS frase”, *NÃO SÃO* exibidos na tela os caracteres digitados. Pressione ENTER para confirmar e continuar.

Enter PEM pass phrase: ➔ Informe uma chave de sua escolha e pressione ENTER. Guarde essa informação para ser utilizada posteriormente.

Verifying – Enter PEM pass phrase ➔ Confirme redigitando a chave de sua escolha e pressione ENTER.

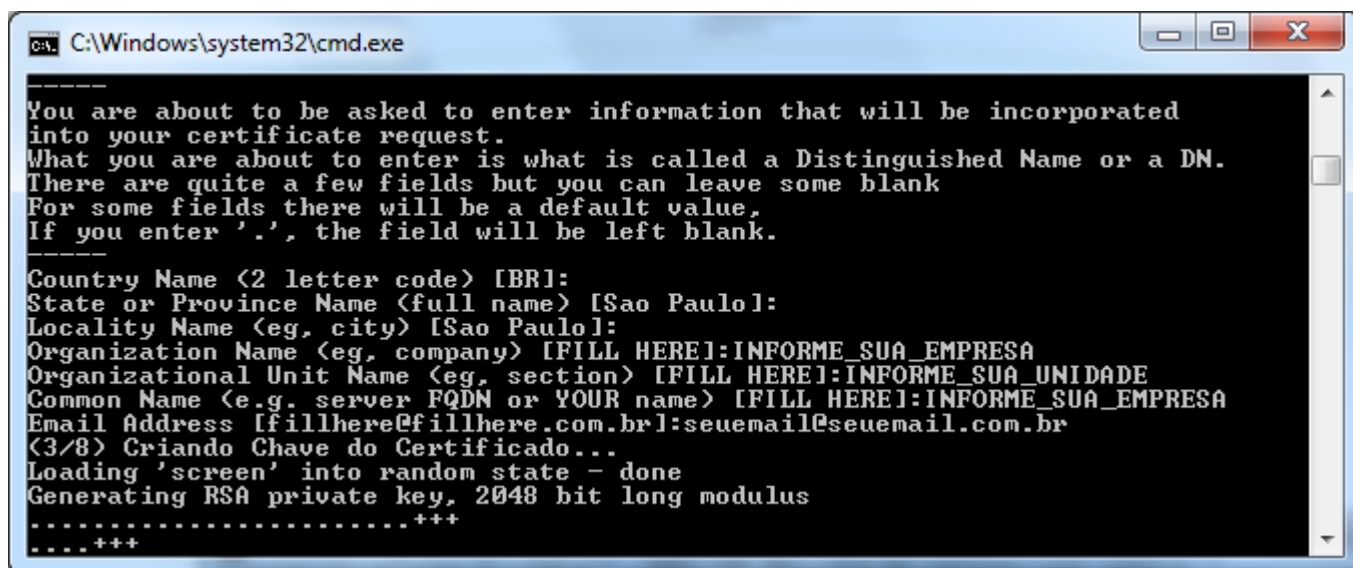


Passo 3/8 : Criando CA (Certificate Authority)

Para geração da CA, serão necessárias as seguintes informações:

- Nome do País
- Estado
- Cidade
- Nome da Organização
- Nome da unidade da organização
- Nome Comum/Fantasia da Organização
- Email

Para manter as informações já presentes apenas pressione “ENTER”.



```
C:\Windows\system32\cmd.exe

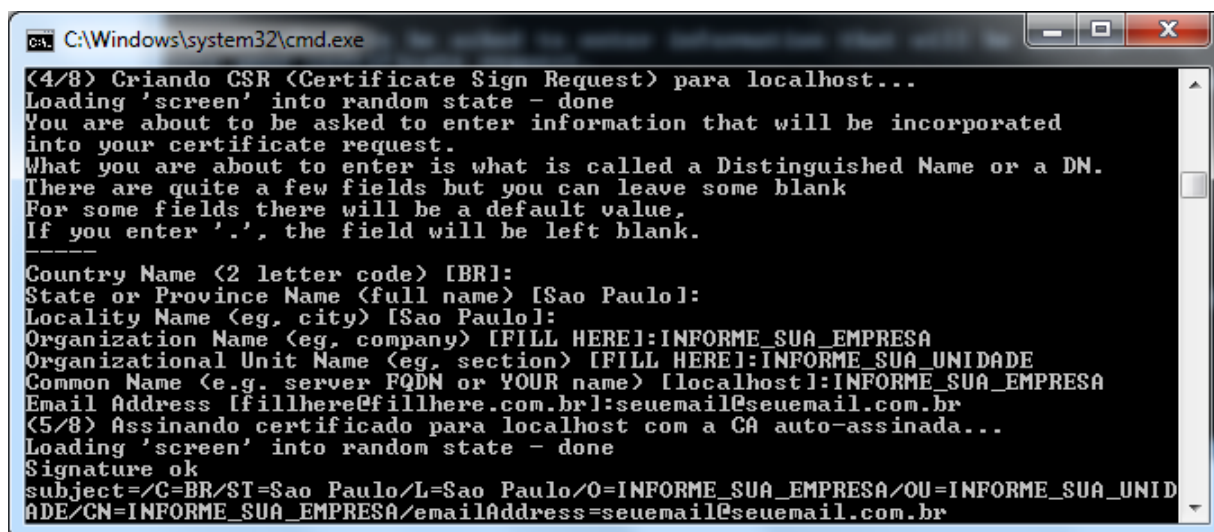
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [BR]:
State or Province Name (full name) [Sao Paulo]:
Locality Name (eg, city) [Sao Paulo]:
Organization Name (eg, company) [FILL HERE]:INFORME SUA EMPRESA
Organizational Unit Name (eg, section) [FILL HERE]:INFORME SUA UNIDADE
Common Name (e.g. server FQDN or YOUR name) [FILL HERE]:INFORME SUA EMPRESA
Email Address [fillhere@fillhere.com.br]:seuemail@seuemail.com.br
(3/8) Criando Chave do Certificado...
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
++++
++++
```

Passo 4/8 : Criando uma CSR (Certificate Sign Request) para localhost

Para geração do certificado assinado, serão necessárias as seguintes informações:

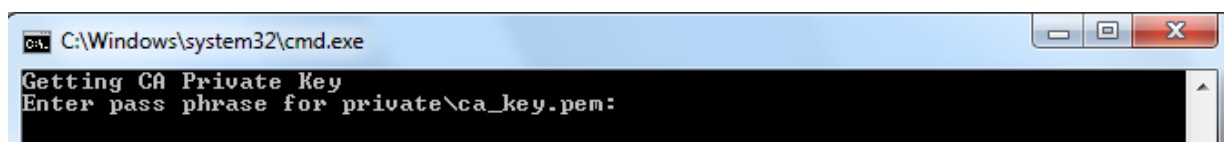
- Nome do País
- Estado
- Cidade
- Nome da Organização
- Nome da unidade da organização
- Nome Comum -> **Neste campo informar “localhost” (pressione ENTER para manter a informação previamente configurada)**
- email



```
C:\Windows\system32\cmd.exe
(4/8) Criando CSR (Certificate Sign Request) para localhost...
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [BR]:
State or Province Name (full name) [Sao Paulo]:
Locality Name (eg, city) [Sao Paulo]:
Organization Name (eg, company) [FILL HERE]:INFORME_SUA_EMPRESA
Organizational Unit Name (eg, section) [FILL HERE]:INFORME_SUA_UNIDADE
Common Name (e.g. server FQDN or YOUR name) [localhost]:INFORME_SUA_EMPRESA
Email Address [fillhere@fillhere.com.br]:seuemail@seuemail.com.br
(5/8) Assinando certificado para localhost com a CA auto-assinada...
Loading 'screen' into random state - done
Signature ok
subject=/C=BR/ST=Sao Paulo/L=Sao Paulo/O=INFORME_SUA_EMPRESA/OU=INFORME_SUA_UNID
ADE/CN=INFORME_SUA_EMPRESA/emailAddress=seuemail@seuemail.com.br
```

Informe a chave privada (a mesma informada anteriormente no passo 2/8)

Enter pass frase for private\ca_key: ➔ Informe sua chave privada e pressione ENTER.



```
C:\Windows\system32\cmd.exe
Getting CA Private Key
Enter pass phrase for private\ca_key.pem:
```

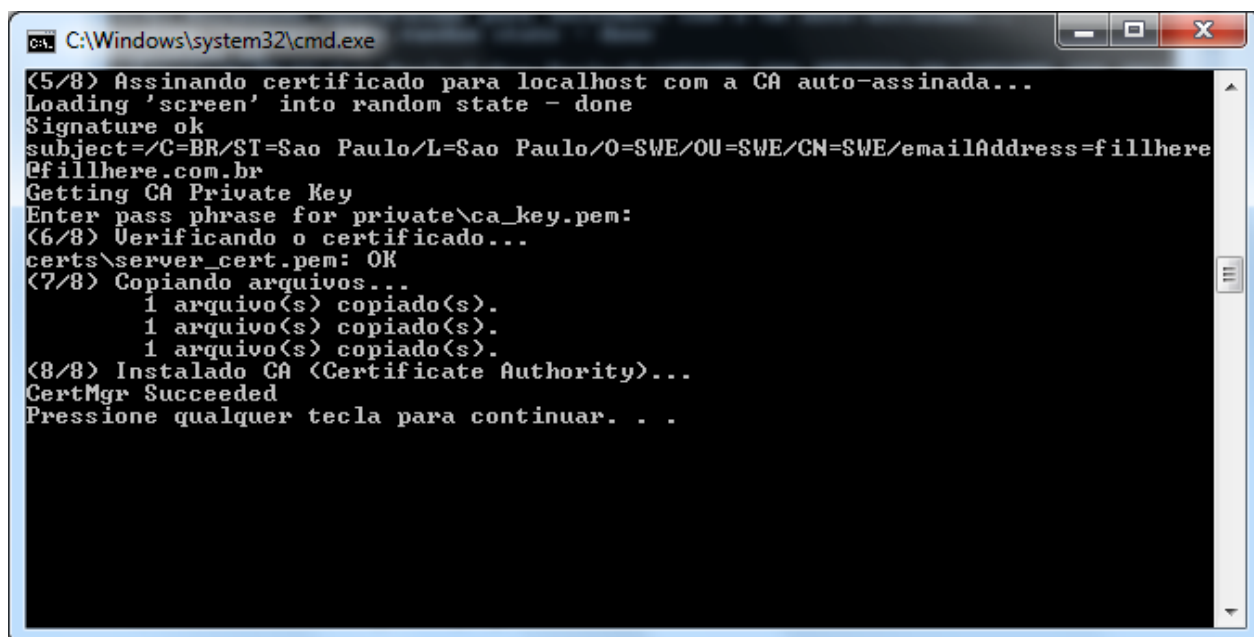
Passo 5/8: Assinando certificado para localhost com a CA auto-assinada

Passo 6/8: Verificando o Certificado

Confirme se neste passo é exibida a seguinte informação na tela: `certs\server_cert.pem: OK`

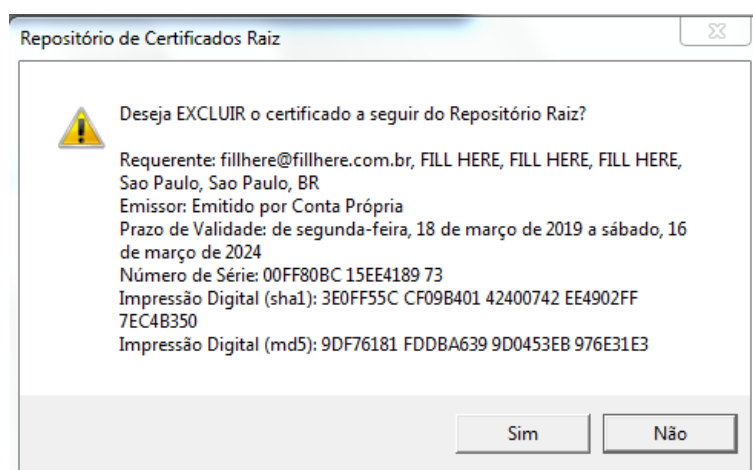
Passo 7/8: Copiando Arquivos

Passo 8/8: Instalando o Certificado (CA)

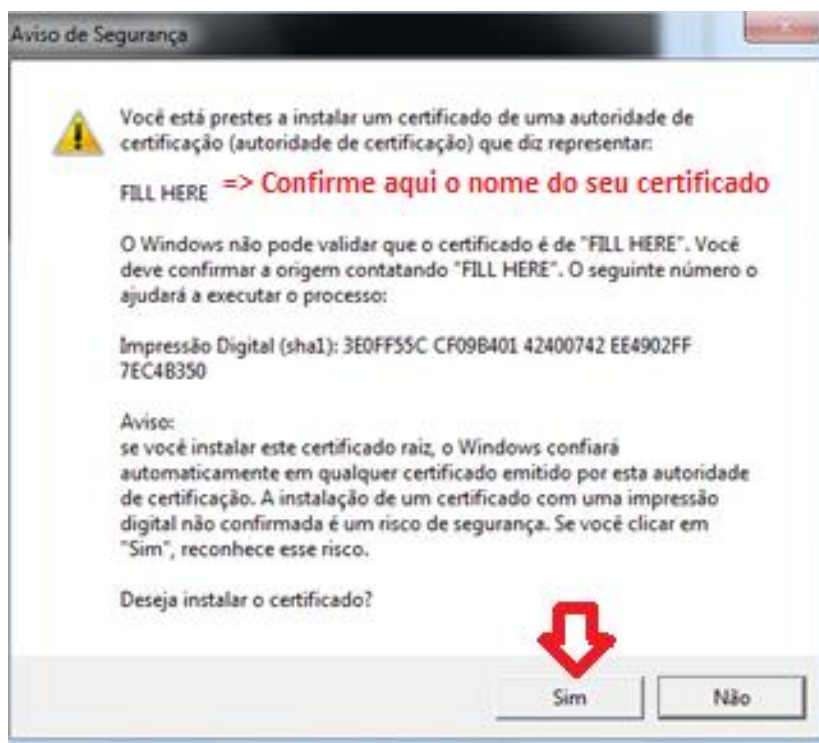


```
C:\Windows\system32\cmd.exe
(5/8) Assinando certificado para localhost com a CA auto-assinada...
Loading 'screen' into random state - done
Signature ok
subject=/C=BR/ST=Sao Paulo/L=Sao Paulo/O=SWE/OU=SWE/CN=SWE/emailAddress=fillhere@fillhere.com.br
Getting CA Private Key
Enter pass phrase for private\ca_key.pem:
(6/8) Verificando o certificado...
certs\server_cert.pem: OK
(7/8) Copiando arquivos...
      1 arquivo(s) copiado(s).
      1 arquivo(s) copiado(s).
      1 arquivo(s) copiado(s).
(8/8) Instalado CA (Certificate Authority)...
CertMgr Succeeded
Pressione qualquer tecla para continuar. . .
```

Durante este passo, caso já exista um certificado da mesma fonte, será questionado se deseja excluir o certificado. Escolha SIM para prosseguir.



Durante este passo você poderá ser questionado se deseja instalar o certificado. Confirme se os dados do certificado questionado são os mesmos do certificado que você gerou e informe "SIM" para prosseguir.



Passo 9/9: Instalando o AgenteClisitef como um serviço do Windows

Nesta etapa o AgenteClisiTef.exe será instalado como um serviço do Windows. Confirme se neste passo é exibida a seguinte informação na tela: “Serviço AgenteClisitef instalado com sucesso”. Ou “Serviço AgenteClisitef atualizado com sucesso”

```
Instalando agenteclisitef.exe como um servico do Windows. A instalacao sera vali  
da apos a reinicializacao do computador.  
Serviço AgenteClisitef instalado com sucesso.  
Pressione qualquer tecla para continuar. . .
```

Para uma primeira utilização do AgenteClisitef o mesmo deverá ser iniciado manualmente. Ou após reiniciar o computador, ele já será executado automaticamente na inicialização do Windows.

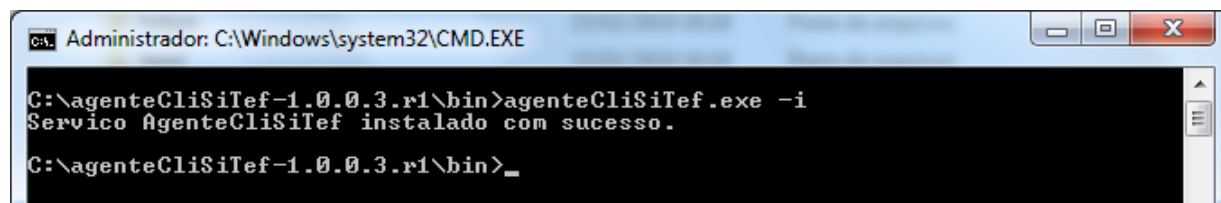
Após estes passos o AgenteClisitef está pronto para integração com a automação.

4.5 Instalando o AgenteClisitef como um serviço do Windows

Esse passo já está sendo realizado no utilitário [gera_certificado.bat](#) e [instala.bat](#), mas caso seja necessário ser utilizado de forma independente, segue instruções de uso:

Através do *prompt* de comando a partir da pasta /Bin, execute o seguinte comando para ativar o AgenteClisitef como um serviço do Windows.

```
C:\agenteCliSiTef\bin> agenteCliSiTef.exe -i
```



Para uma primeira utilização do *AgenteClisitef* o mesmo:

- poderá ser iniciado manualmente; OU
- poderá ser iniciado executando o comando `net start AgenteCliSiTef` no prompt de comando; OU
- após reiniciar o computador, ele já será executado automaticamente na inicialização do Windows.

Após estes passos o *AgenteCliSiTef* está pronto para integração com a automação.

4.6 Criando um pacote *master* para instalação em estações de trabalho

Após a realização dos itens descritos acima no capítulo 4, recomendamos criar um pacote para distribuição e instalação nas demais estações de trabalho (PDV's). Este procedimento visa facilitar as demais instalações onde não será mais necessário gerar os certificados do *openSSL*.

Utilize o utilitário "**gera_pacoteMaster.bat**" que irá gerar na pasta raiz do pacote do *AgenteCliSiTef* a pasta "**deployAgenteClisitefMaster**". Esta pasta poderá ser replicada nas demais estações de trabalho/PDV's.

Por segurança, os arquivos de configuração do certificado foram removidos desta pasta, podendo ser replicada.

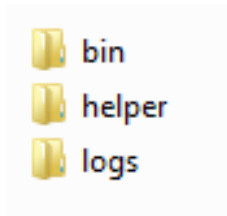
Após os procedimentos acima, o pacote para instalação das demais máquinas está disponível "**deployAgenteClisitefMaster**" e pode ser distribuído. Compacte-o com o software compactador de sua preferência.



Atenção: O pacote original deve ser mantido para seu controle e manutenção dos certificados, porem para distribuição você deverá utilizar a pasta "**deployAgenteClisitefMaster**".

5 Instalação em estações de trabalho com pacote *master*

Passo 1/2: Descompacte o pacote *master*.



Passo 2/2: Execute o script *instala.bat*.

Acesse a pasta /helper e execute o utilitário “*instala.bat*”. Execute como Administrador (clique com o botão direito e escolha opção “Executar como Administrador”). Este utilitário instala o certificado da CA, instala o *AgenteCliSiTef.exe* como um serviço do Windows e inicia o serviço.

Após estes passos o *AgenteClisitef* está pronto para integração com a automação.

6 Gerenciamento dos Certificados

A responsabilidade de gerar e gerenciar os certificados necessários para conexão SSL é do cliente. Os parâmetros podem ser alterados nos arquivos presentes na pasta /helper.

Na configuração atual os certificados serão gerados com uma validade de 5 anos. Esta e outras configurações podem ser customizadas e são responsabilidade do cliente.

Para alterar o tempo de validade dos certificados ajuste conforme necessário o parâmetro “-days 1825” presente no arquivo **gera_certificados.bat** (linhas 13 e 22).

7 Histórico de Alterações

Data	Autor	Versão	Descrição
15/02/2019	Ana Paula Londino	1.00	Versão Inicial deste documento.
26/02/2019	Ana Paula Londino	1.01	<ul style="list-style-type: none">Inclusão de informações referente a opção do download do GnuWin32Correção da informação Common name a ser informada na geração do CSR (localhost)
18/03/2019	Ana Paula Londino	1.02	<ul style="list-style-type: none">Adicionado Box de informações referente a digitação da chave privada para gerar o certificado.Ajustes nos utilitários que passaram a já executar a instalação do AgenteCliSitef.exe como um serviço do Windows.
03/04/2019	Leo Ueda	1.03	<ul style="list-style-type: none">Simplificação da instalação do pacote master (agora é necessário apenas executar o instala.bat). Corresponde à versão 1.0.0.5.r1.