PRODIST®

Manual do Usuário

Secure Transaction System RSFN

(STS RSFN 5.2)

Outubro 2014

Versão 5.2

REVISÃO

Data	Autor
11-01-2012	Renato Koeke
30-01-2012	Fernando Tasso
12-12-2012	Renato Koeke
07-10-2013	Renato Koeke

SUMÁRIO

1 Introdução

Este documento descreve os procedimentos de instalação e administração do **Secure Transaction System RSFN (STS - RSFN)** e, caso você não esteja familiarizado com o produto e seus antecessores, deve ser lido em sua integridade antes da instalação dos componentes da solução.

2 Componentes do pacote de instalação

O pacote de instalação é composto dos seguintes arquivos:

- **{STS RSFN Setup.exe}** - este arquivo possui todos os componentes necessários para a instalação dos módulos **Cliente e Servidor STS.**
- **Arquivo de licença** - este arquivo de sufixo **".lic"** é enviado pela **PRODIST** junto com o **{STS RSFN Setup.exe}**.

3 Requisitos Mínimos e Recomendações

Os seguintes requisitos devem ser observados antes de iniciar o procedimento de instalação e configuração do Servidor e do Cliente STS:

- Hardware mínimo: Máquina com processador Pentium IV ou superior, 1GB de Memória RAM e monitor configurado para resolução mínima de 800 X 600 pixels.
- STS Servidor: Sistema Operacional Windows 2003 ou Superior.
- STS Cliente Windows: Sistema Operacional Windows 2003 ou Superior.
- STS Cliente Java: Qualquer sistema operacional com SUN JAVA (J2SE 5 ou superior)
- O usuário deverá estar autenticado em uma sessão com privilégios de Administrador do servidor.

O STS RSFN v5.2 é um sistema de 32 bits (x86) mas pode ser instalado em sistemas Windows de 64 bits (x64).

Observação: Quando estiver fazendo um upgrade de versão, atualize sempre os aplicativos "Parâmetros do Cliente STS" e "Parâmetros do Servidor STS" do STS.

4 Arquitetura da solução

Os dois principais componentes da solução **STS** são o `STSClient.exe` e o `STSServer.exe`. Estes componentes são instalados como serviços do Windows e após a instalação estarão presentes no diretório **`%WINDIR%/system32`** ou **`%WINDIR%/SysWOW64.`**

O **Servidor STS (`STSServer.exe`)** é uma aplicação *multi-thread* capaz de processar até 2000 (este fator depende muito do hardware utilizado) conexões simultâneas. Embora seja possível abrir apenas uma conexão entre o sistema legado (Ex.: Mensageria) e o **Servidor STS**, para obter altas taxas de desempenho é necessário que o sistema legado abra múltiplas conexões com o **Servidor STS.** Uma abordagem de conexão única, entre o legado e o **Servidor STS**, é a forma mais simples de integração e irá funcionar normalmente, sendo uma alternativa bastante eficiente se o volume de transações não for alto.

Os parâmetros de configuração do **Cliente STS** são armazenados em um arquivo criptografado denominado **`{Politicamsg.xml}`**, que pode ser atualizado pelo aplicativo **<Parâmetros do Cliente STS>.**

Os parâmetros de configuração do **Servidor STS** são armazenados no arquivo criptografado **`{Politica.xml}`**, que pode ser atualizado pelo aplicativo **<Parâmetros do Servidor STS>.**

O Funcionamento completo é de simples entendimento e está descrito nos passos a seguir:

1. O aplicativo legado (Ex.: Mensageria) faz chamadas a uma das aplicações **Cliente STS** (Java ou Windows) e esta se encarrega de encaminhar tais requisições ao **Servidor STS**, através de uma conexão *TCP Sockets*. Todo o processo de comunicação entre o Cliente e o Servidor, incluindo procedimentos de *Failover* e *Load Balance* é tratado pela aplicação **Cliente STS** invocada.
2. O **Servidor STS** recebe o pedido de criptografia (ou decriptografia) e executa a função adequada, conforme definido no manual de segurança do BACEN ou da CIP. O resultado do tratamento é devolvido ao legado através da aplicação **Cliente STS**, utilizando a conexão *TCP Sockets* que por ela foi iniciada.
3. Em caso de falha, o código de erro correspondente é retornado ao legado pela aplicação **STS Client**.

5 Procedimentos de Instalação

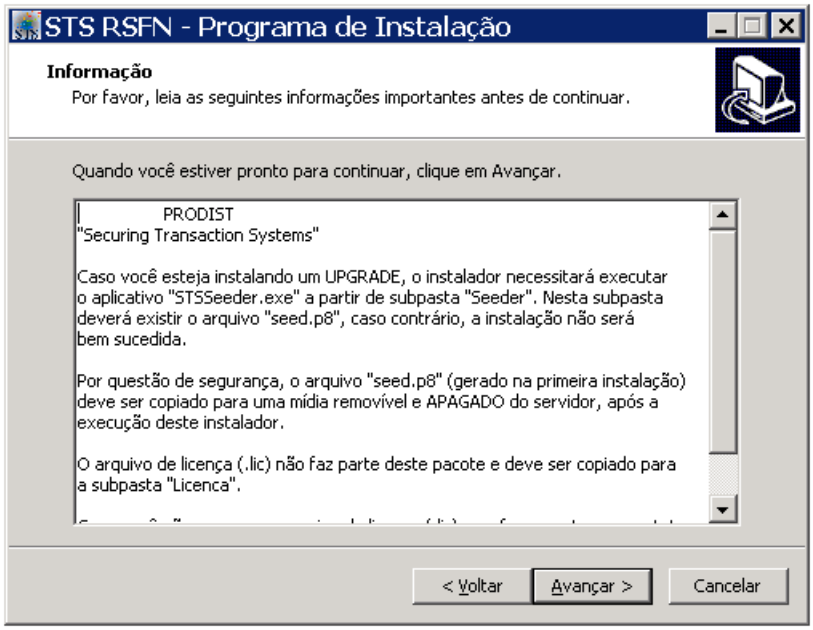
5.1 INSTALAÇÃO DO PACOTE STS

Os procedimentos de instalação do STS estão descritos a seguir. É necessário ter privilégios de administrador na máquina onde o serviço será instalado. É importante frisar que todos os passos são **obrigatórios** e devem ser executados **na ordem** apresentada abaixo:

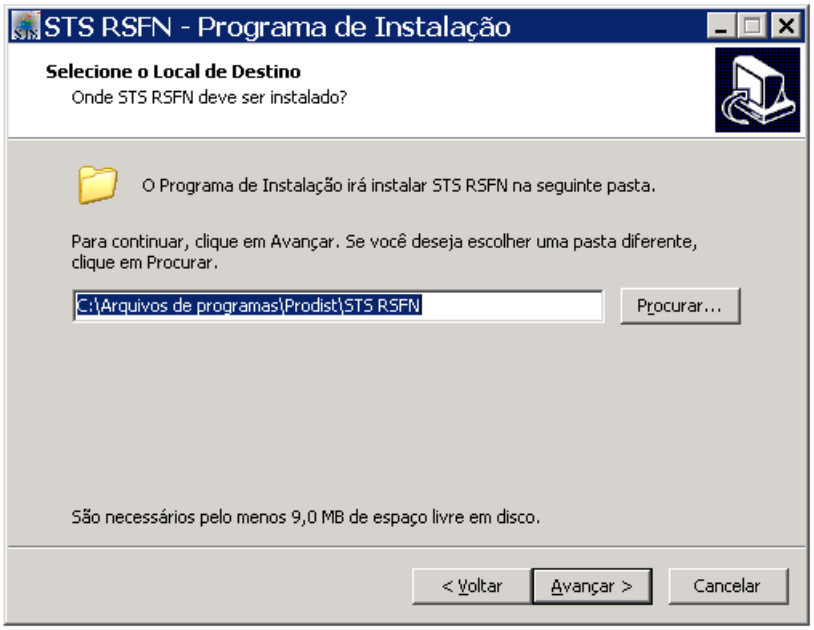
a) Copie o arquivo **{STS RSFN Setup.exe}** para um diretório temporário na máquina onde será instalado o serviço de criptografia.

b) Dê um duplo clique sobre o aplicativo **{STS RSFN Setup.exe}**. Neste momento a instalação será iniciada e será apresentada a seguinte janela:

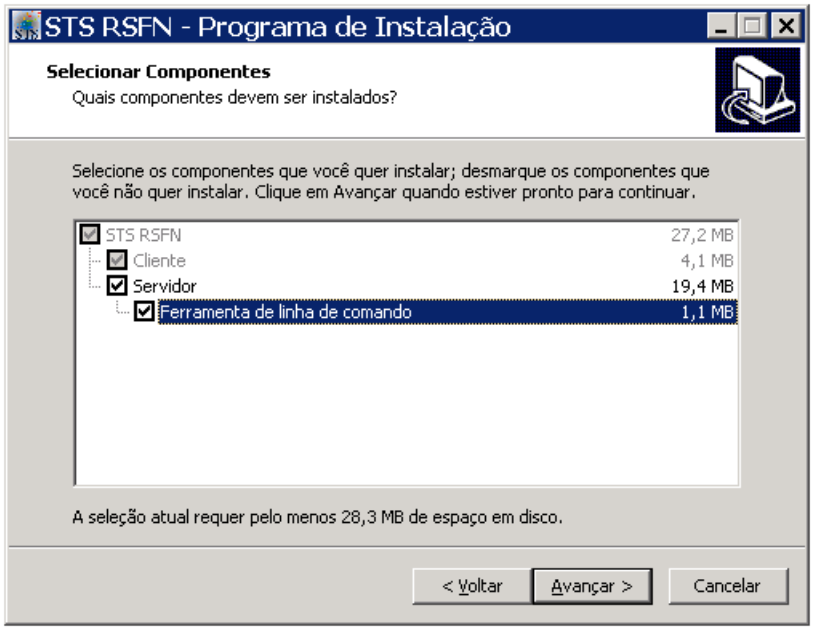
c) Clique em **Avançar** para continuar e uma janela com informações importantes será exibida. Leia com atenção e em seguida clique em **Avançar**.



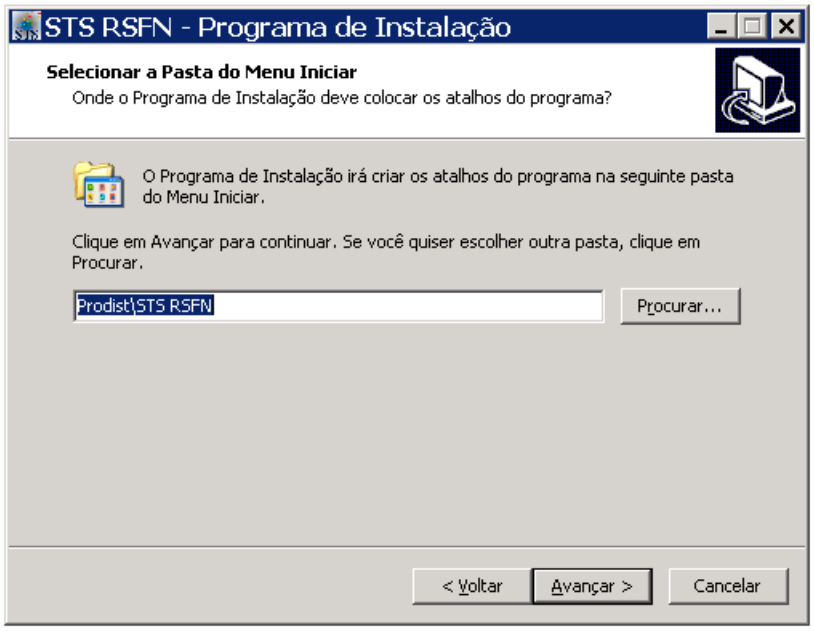
d) Na janela seguinte escolha o local para a instalação dos arquivos e mais uma vez clique em **Avançar**.



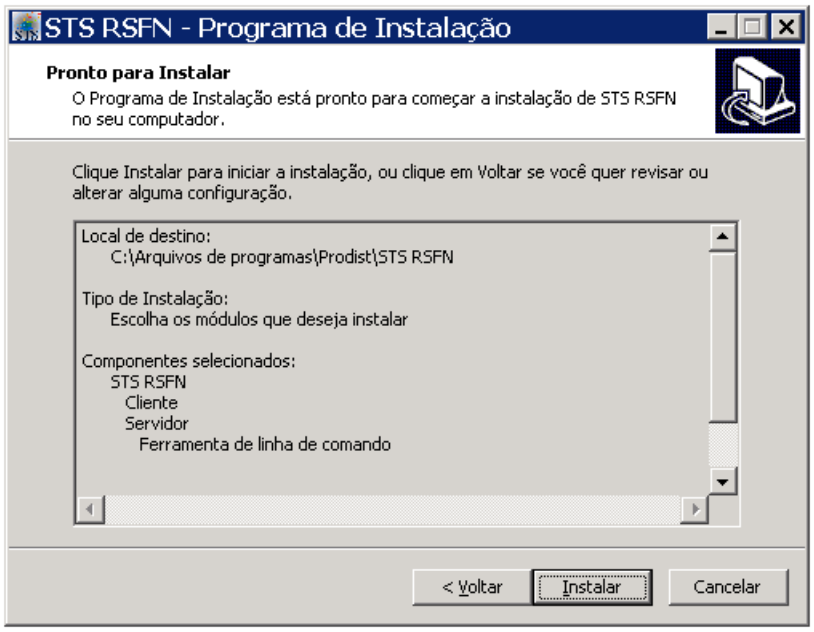
e) Escolha os componentes que deseja instalar. Você pode optar por instalar apenas o **Cliente STS** ou o pacote completo (**Cliente e Servidor STS**). Em seguida, clique em **Avançar**.



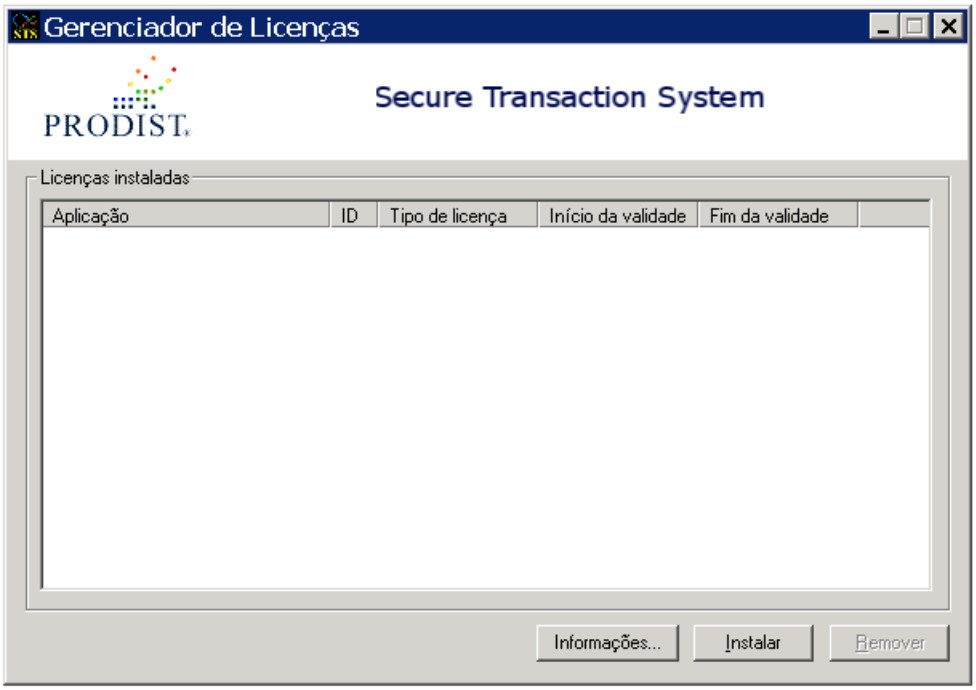
f) Escolha a pasta do **Menu Iniciar** onde deseja instalar o produto. Seguiremos com o exemplo de uma instalação padrão. Em seguida, clique em **Avançar** para dar continuidade.



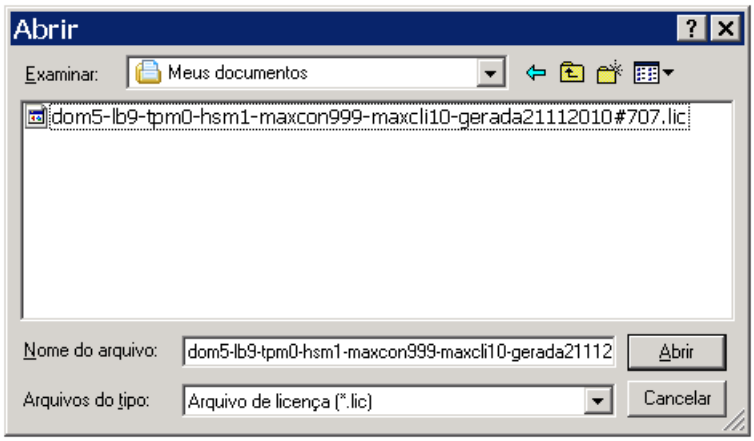
g) Após conferir as opções escolhidas na janela a seguir, clique no botão **Instalar** para que a instalação seja iniciada ou no botão **Voltar** para fazer as correções necessárias.



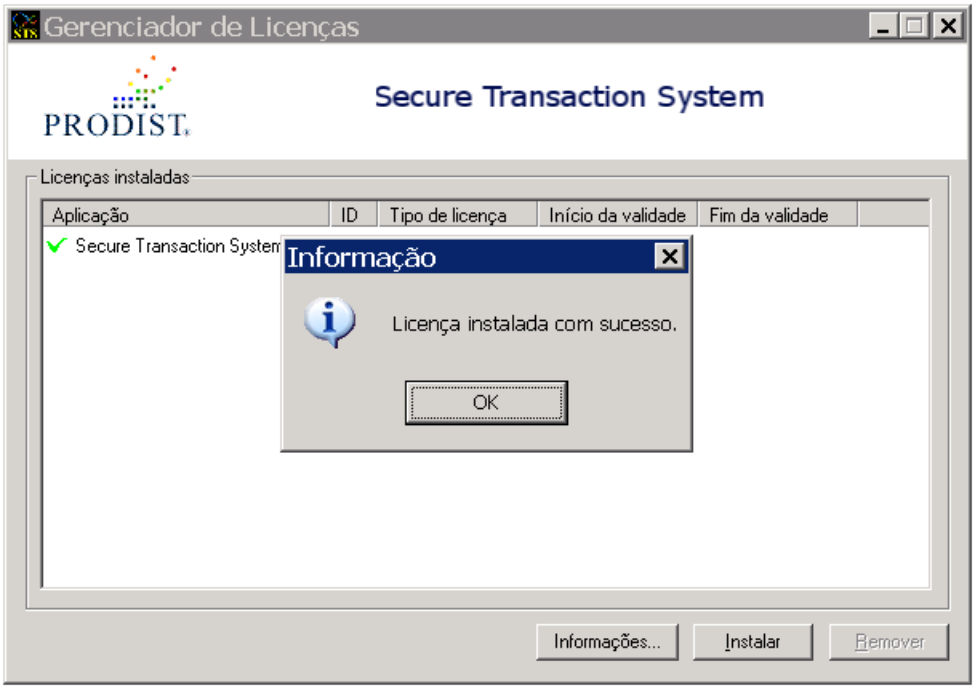
h) Os arquivos serão copiados e os componentes selecionados do STS serão instalados. Caso ainda não haja uma licença instalada, será solicitado ao usuário que cadastre uma licença (arquivo **"`.lic`"** fornecido pela **PRODIST**) do produto. Se a janela já mostrar uma licença anteriormente instalada e você desejar mantê-la, clique em **[X]** para fechar a janela e vá para o passo (k).



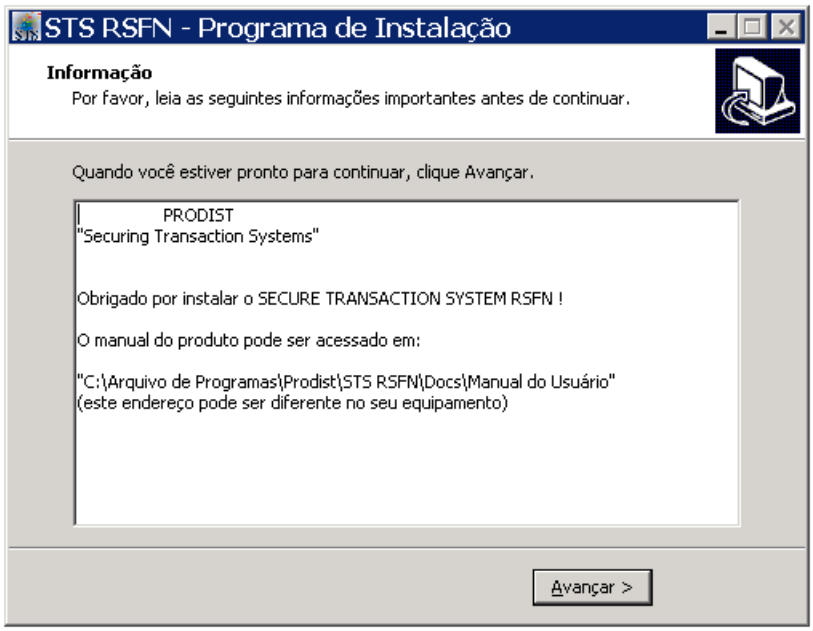
i) Clique no botão **Instalar** e através da janela a seguir, selecione o arquivo que contém a licença fornecida pela **PRODIST**.



j) O sistema irá informar quando a instalação da licença for concluída. Após a licença ter sido instalada, clique no botão **OK.**



k) Em seguida clique em **Avançar**.



l) E depois clique em **Concluir** para finalizar a instalação

ATENÇÃO: Caso você tenha optado por instalar o componente **Cliente STS** em uma máquina fisicamente separada do **Servidor STS** (como mostra o procedimento **(e)**), certifique-se de que a **data e a hora entre eles esteja sincronizada**.

5.1.1 Instalando o STS em outros equipamentos que precisem utilizar as mesmas chaves privadas (ex: servidores de Load Balance e/ou Failover)

1. Se a sua instalação utiliza HSM (Hardware Security Module), instale primeiro o driver do HSM.
2. Instale o pacote **{STS RSFN Setup.exe}**.
3. Copie os arquivos **{vault.sts}** e **{politica.xml}** da pasta **{Prodist\STS RSFN\Servidor}** do primeiro equipamento para a pasta correspondente no segundo equipamento.
4. Copie também o arquivo **{seed.p8}** da pasta **{Prodist\STS RSFN\Seeder}** do primeiro equipamento para a pasta correspondente no segundo equipamento.
5. Copie o arquivo executável **{STSServer.exe}** da pasta **{Windows\System32} (32 bits)** ou **{Windows\SysWOW64} (64 bits)** do primeiro equipamento para a pasta correspondente no segundo equipamento.

6. Se as chaves privadas estiverem em um **HSM nCipher**, copie os arquivos da pasta **{\nfast\KMData\}** do primeiro equipamento para a pasta correspondente no segundo equipamento.
7. Se as chaves privadas não estiverem em HSM, sobrescreva a pasta **{Prodist\STS RSFN\Servidor\Vault\}** no segundo equipamento com a pasta correspondente do primeiro equipamento.
8. Sobrescreva a pasta **{Prodist\STS RSFN\Servidor\Certificados\}** no segundo equipamento com a pasta correspondente do primeiro equipamento.

5.1.2 Procedimento para upgrade de novas versões do Servidor STS

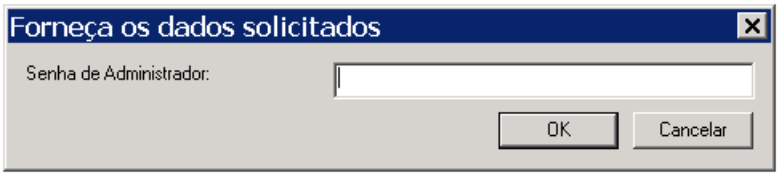
Para realizar o upgrade para novas versões do Servidor STS, proceda da seguinte maneira:

1. Tenha certeza de possuir os arquivos **{seed.p8}** e **{vault.sts}** da instalação atual.
2. Faça um backup da pasta **{PRODIST\STS RSFN}** do equipamento onde o upgrade será realizado e dos arquivos **{APICripto.dll}**, **{APILdap.dll}**, **{APIVaultSTS.dll}** e **{STSServer.exe}**.
3. Pelo Painel de Controle do Windows, desinstale o pacote do **<STS RSFN>** atual.
4. Instale o novo pacote do **<STS RSFN>**.

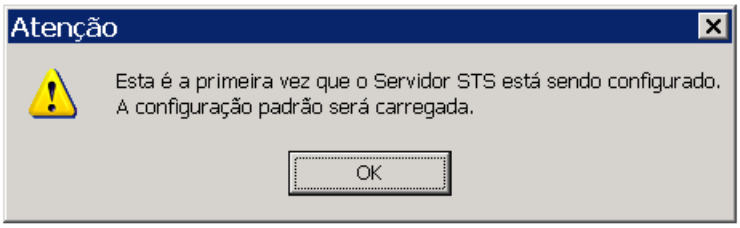
5.2 CONFIGURANDO O SERVIDOR STS

Execute o aplicativo **<Parâmetros do Servidor STS>** clicando em **Iniciar > Todos os Programas > Prodist > STS RSFN > Servidor > Parâmetros do Servidor STS.**

Para acessar o aplicativo será necessário digitar a senha de acesso (1234 por padrão).



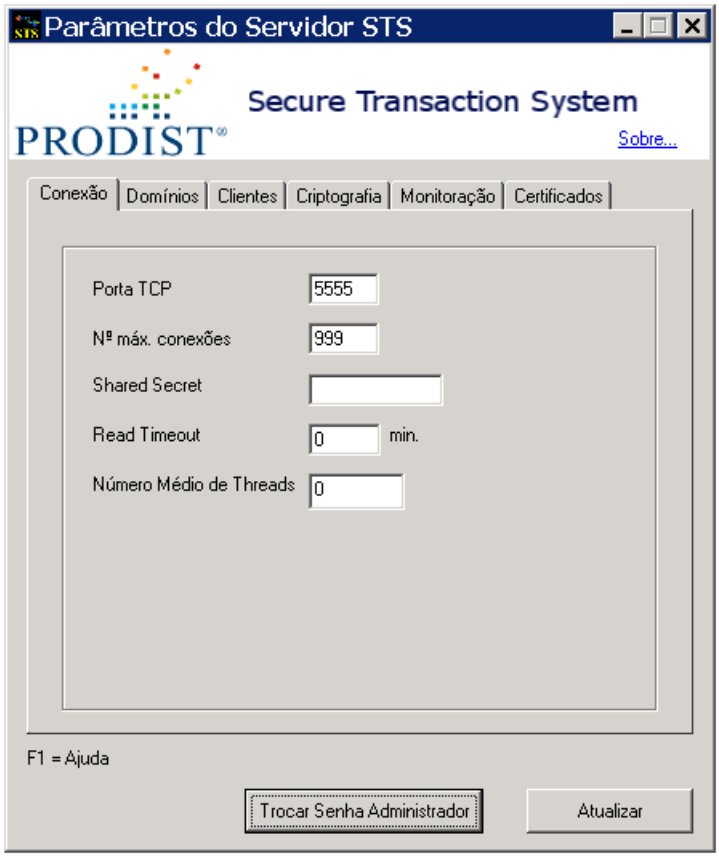
Na primeira vez que você executar este aplicativo receberá uma mensagem indicando que a configuração padrão será carregada. Clique no botão **[OK]**.



Após a abertura da janela de configuração, altere os valores dos parâmetros do Servidor STS de acordo com as necessidades de seu ambiente. Tenha em mente que os valores padrão sugeridos são os mais adequados para a grande maioria dos casos.

Obs.: Se for a primeira vez que você utiliza este aplicativo, **não configure as Abas <Criptografia>** e **<Certificados>**. Os parâmetros destas abas serão abordados mais adiante.

5.2.1 Aba <Conexão>



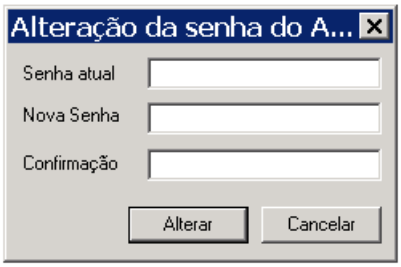
- Parâmetro "**Porta TCP**": Este campo deverá ser preenchido com o número da porta TCP a ser utilizada para comunicação entre o **Servidor STS** e os **Clientes STS**. Lembre-se que você precisa configurar o mesmo número da porta no Servidor e nos

Clientes STS. Os valores possíveis para este campo estão na faixa de 1 a 65535. O valor padrão é 5555.

- Parâmetro "**Nº máx. conexões**": Este campo deverá ser preenchido com o número máximo de conexões simultâneas que serão aceitas pelo **Servidor STS** para tratamento de pedidos de criptografia e decriptografia oriundos de **Clientes STS**. Os valores possíveis para o campo estão na faixa de 1 a 2000. O valor padrão é 999.
- Parâmetro "**Shared Secret**": Este campo deverá ser preenchido com uma senha que tem por objetivo autenticar a conexão do **Cliente STS** com o **Servidor STS**. A senha configurada nesta caixa diferencia caracteres maiúsculos de minúsculos e deve ser composta de no mínimo 8 (oito) e no máximo 36 (trinta e seis) caracteres. O **Servidor STS** só aceitará conexões de **Clientes STS** que forneçam esta senha.
- Parâmetro "**Read Timeout**": Este campo deverá ser preenchido com o tempo máximo, em minutos, que um **Cliente STS**, após ter iniciado uma conexão com o **Servidor STS**, poderá ficar inativo. Ou seja, o tempo máximo que o **Servidor STS** irá aguardar, em cada conexão aberta por algum **Cliente STS**, por um pedido de criptografia/decriptografia. Se o **Servidor STS** detectar que algum **Cliente STS** atingiu o limite máximo de inatividade estabelecido por este parâmetro, ele irá, unilateralmente, fechar aquela conexão.

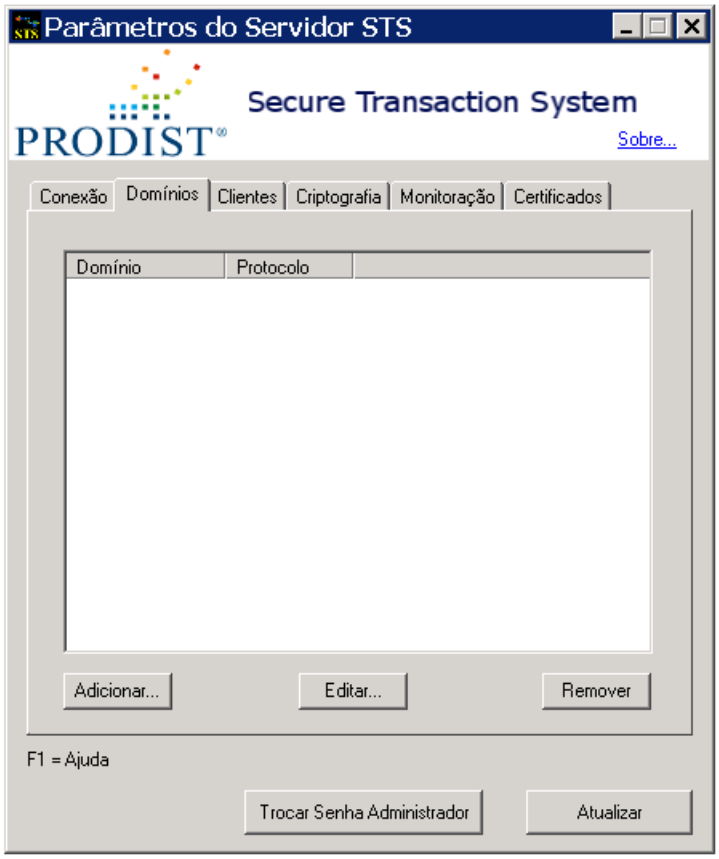
  O objetivo deste parâmetro é evitar que o servidor fique com muitas conexões inativas, gastando recursos desnecessariamente. Para configurar um tempo de inatividade ilimitado, preencha este campo com o valor "0". O valor padrão é "0" e este valor é adequado para a maior parte das implantações de **Servidores STS**, especialmente aquelas que processem baixos volumes de transações.
- Parâmetro "**Número Médio de Threads**": Este campo deverá ser preenchido com o número médio de threads que devem estar abertas durante a execução normal do STS. Sempre que o sistema chegar ao dobro deste valor, ele passará a trabalhar em "**Modo de Alerta**". O "**Modo de Alerta**" é um modo que gera mais informações de *debug* nos arquivos de log. O valor máximo para este campo é 2000 e o valor 0 (zero) indica que este teste não deve ser realizado. O valor padrão para este parâmetro é 0 (zero), sendo adequado para a maior parte das implementações de **Servidores STS**.
- Botão **[Trocar Senha Administrador]**: Utilize este botão para alterar a senha do administrador STS.

  A senha padrão é 1234.



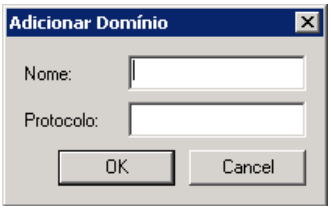
- Botão **[Atualizar]**: Utilize este botão para salvar as novas configurações do **Servidor STS**.

5.2.2 Aba <Domínios>



- Nesta Aba você deve cadastrar os domínios para os quais irá solicitar operações de criptografia. Cada domínio tem seu próprio conjunto de certificados de participantes e suas próprias chaves privadas, sendo que somente uma chave privada poderá estar ATIVA por domínio.
- Você não pode criar par de chaves, ou importar chave privada, sem antes ter criado o domínio sob o qual elas deverão estar cadastradas.

- Ao cadastrar um domínio você precisará escolher qual a versão do Protocolo de Segurança que este domínio deverá considerar, para o processamento dos dados. Atualmente existem duas versões do Protocolo de Segurança, sendo que:
  - A versão 1 só aceita chaves privadas e certificados de 1024 bits e em cada mensagem processada agrega um Header (cabeçalho) de 332 bytes.
  - A versão 2 aceita chaves privadas de 1024 bits ou 2048 bits e certificados dos dois tamanhos e em cada mensagem processada agrega um Header de 588 bytes.
- Clique no botão **[Adicionar]** para criar um domínio de pares de chaves (privadas e públicas) e certificados, que serão utilizados pelo **Servidor STS** durante o processamento das mensagens. É obrigatório criar pelo menos um domínio para que seja permitida a inclusão de **Clientes STS** na lista de clientes autorizados. Após clicar a seguinte janela será exibida:



Uma breve descrição dos campos a preencher está apresentada a seguir:

- Parâmetro "**Nome**": Em geral, um nome de domínio está associado ao tipo de sistema que será atendido pelo STS. Digite o nome do domínio com até 5 caracteres. Sugerimos utilizar nomes em formato similar a:

  "STR00", "MES00", "SCG00", "CCC00", etc...

- Parâmetro "**Protocolo**": Este parâmetro determina de que maneira o Servidor STS deverá se comportar, em relação à versão do protocolo de criptografia a ser considerada para o tratamento dos pacotes. As opções disponíveis são "**1**" ou "**2**".

  Se for escolhida a **versão 1** do protocolo de segurança, o STS irá processar todos os pacotes recebidos, de acordo com as especificações do ***Manual de Segurança do BACEN versão 2.5 (Novembro de 2009)***. Se for escolhida a **versão 2** do protocolo de segurança, o STS irá processar todos os pacotes recebidos, de acordo com as especificações do ***Manual de Segurança do BACEN versão 3.0 (Março de 2011)***.

Obs.: Na **versão 1**, o STS irá produzir assinaturas RSA 1024 com *hash* SHA-1 e só irá aceitar pacotes de outras instituições que tenham sido gerados com este mesmo tipo de assinatura.
Já na **versão 2**, o STS poderá produzir assinaturas RSA 1024 com *hash* SHA-256 ou assinaturas RSA 2048 com *hash* SHA-256. Na **versão 2**, serão aceitos pacotes de outras instituições que tenham sido gerados com assinatura RSA 1024 e *hash* SHA-1, RSA 1024 e *hash* SHA-256 e pacotes gerados com assinatura RSA 2048 e *hash* SHA-256.

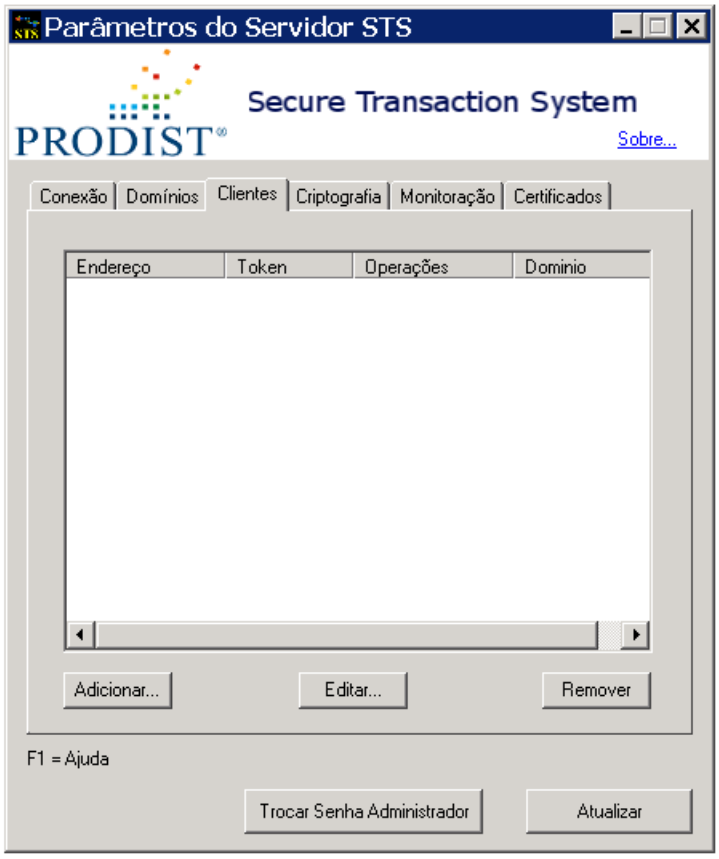
Um mesmo domínio não pode suportar mais de um tipo de protocolo.

- Selecione um domínio existente e clique no botão **[Editar]** para alterar seu nome e/ou a versão do protocolo de segurança associado a ele.

- Selecione um domínio existente e clique no botão **[Remover]** para exclui-lo.

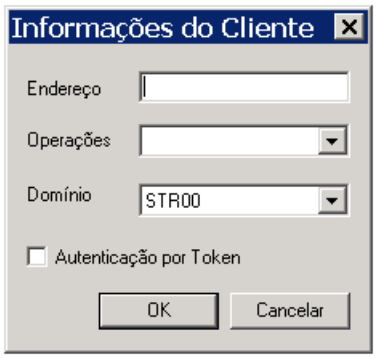
Observação: Alterar um nome de domínio ou removê-lo não gera nenhuma ação sobre os objetos das pastas de instalação do produto, ou sobre o conteúdo dos HSMs. Toda a movimentação de arquivos necessária para refletir um desses tipos de ação deverá ser executada manualmente pelo usuário.

5.2.3 Aba <Clientes>



- Esta Aba apresenta a lista de "**Clientes Autorizados**" a requisitar operações de criptografia contra o **Servidor STS**. Ela deverá ser preenchida com os endereços IP dos **Clientes STS** autorizados.

Para autorizar um novo **Cliente STS**, clique no botão **[Adicionar]** e a seguinte janela será exibida:

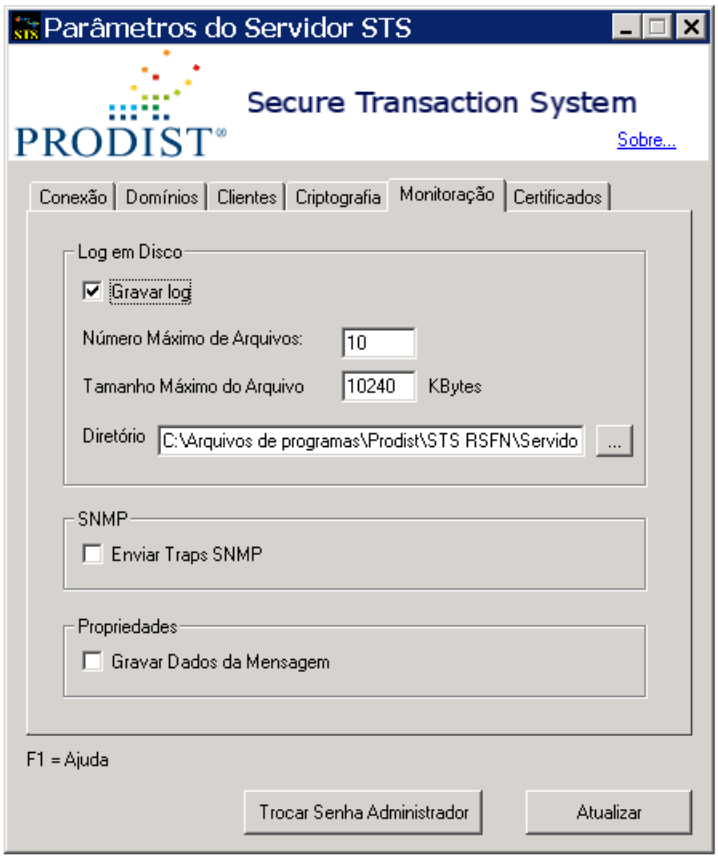


- Parâmetro **"Endereço"**: Endereço IP ou UNC ou Alias DNS (`192.168.60.1`, `STSServer` ou `mensageria.banco.com.br`) do **Cliente STS** a ser autorizado.

- Caixa **"Operações"**: Operações que o **Cliente STS** está autorizado a realizar. As opções possíveis são: Criptografia, Decriptografia e Todas (Criptografia e Decriptografia);
- Caixa **"Domínio"**: Refere-se ao nome de domínio para o qual o **Cliente STS** poderá requisitar serviços.
- Caixa **"Autenticação por Token"**: Indica se o cliente tem que estar autenticado via Token USB (conforme item 5.6) para ter acesso ao **Servidor STS**. Esta opção só está disponível para **Cliente STS** Windows. **Inicialmente deixe esta caixa desmarcada**.

Obs.: A qualquer momento você pode alterar as configurações de um **Cliente STS** cadastrado. Para editar as configurações de um **Cliente STS**, selecione-o na lista e clique no botão **[Editar]**. Para remover um **Cliente STS** da lista de clientes autorizados, selecione-o na lista e clique no botão **[Remover]**.

5.2.4 Aba <Monitoração>



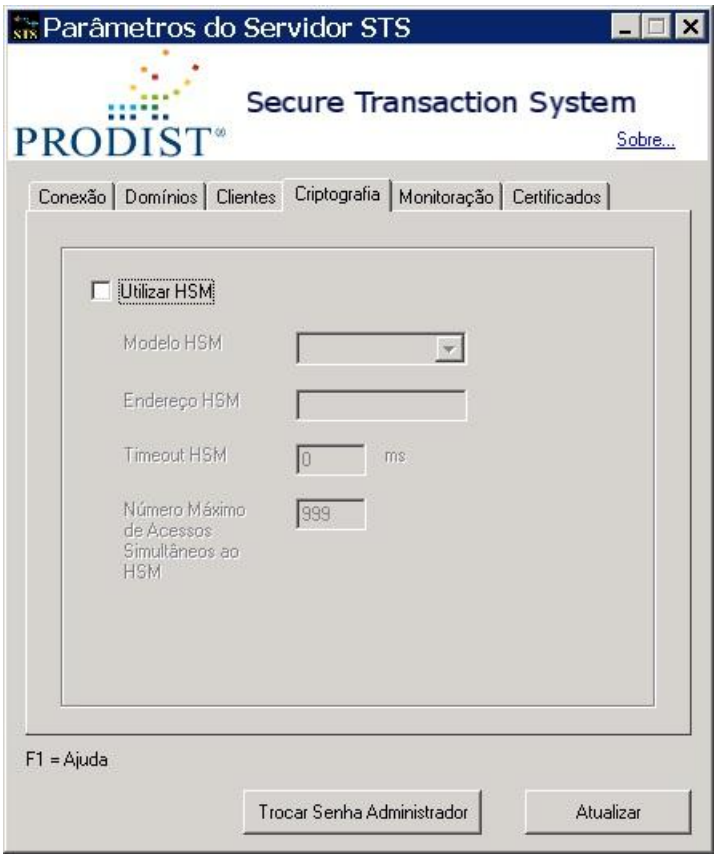
- Caixa "**Gravar Log**" (Log): Esta caixa deverá ser marcada para habilitar a gravação de arquivos de Log pelo **Servidor STS**. Ao marcar esta caixa os campos "N.º Máximo de Arquivos", "Tamanho Máximo do Arquivo" e "Diretório" serão habilitados.
- Parâmetro "**N° Máximo de arquivos**" (Log): Este campo deverá ser preenchido com o número máximo de arquivos de LOG que poderão existir na pasta indicada na caixa "Diretório". No mínimo haverá 1 e no máximo 100 arquivos.
- Parâmetro "**Tamanho Máximo do Arquivo**" (Log): Deverá ser preenchido com o tamanho máximo dos arquivos de LOG. Os valores permitidos variam de 512 a 51200 Kbytes. Ao atingir o tamanho máximo de um arquivo de LOG o **Servidor STS** irá, sucessivamente, abrir outro arquivo. Quando o número máximo de arquivos de LOG for atingido o arquivo mais antigo será apagado e um novo arquivo será criado.

Atenção: Caso o tamanho de um pacote recebido seja superior ao tamanho máximo do arquivo de LOG, o tamanho máximo do arquivo passará a ser igual ao tamanho do pacote, ignorando-se o valor configurado. Isso ocorre para que o pacote não seja partido, no momento em que o LOG for gerado.

- Parâmetro "**Diretório**": Este campo deverá ser preenchido com o nome da pasta onde os arquivos de Log serão criados. Se você pretende que a pasta esteja alocada em algum outro ponto da rede, lembre-se que deverá utilizar um caminho do tipo UNC. Por exemplo: **"\\servidor\certificados".** Nestes casos, o serviço **<STSServer RSFN>** não poderá ser executado sob o usuário **SISTEMA** (**SYSTEM**), que é o usuário de execução da instalação padrão. Será preciso alterar as configurações de execução do serviço, de forma que as credenciais de (logon) execução sejam credenciais de usuário local ou do domínio, com permissão de escrita e leitura no diretório informado, maiores informações de como realizar essa alteração são encontradas no **Apêndice D - Alterando a configurações de execução do serviço STS RSFN.**
- Caixa "**Gravar Dados da Mensagem**": Esta caixa deverá ser marcada se você desejar que o corpo da mensagem (com os dados da transação) também seja gravado no arquivo de Log. Caso essa caixa esteja desmarcada (opção padrão), apenas os cabeçalhos das mensagens serão gravados no arquivo de Log. Isso diminui sensivelmente a quantidade de espaço ocupado pelo arquivo de Log.
- Caixa "**Enviar Traps SNMP**": Esta caixa deverá ser marcada se você deseja que o servidor passe a gerar eventos SNMP.

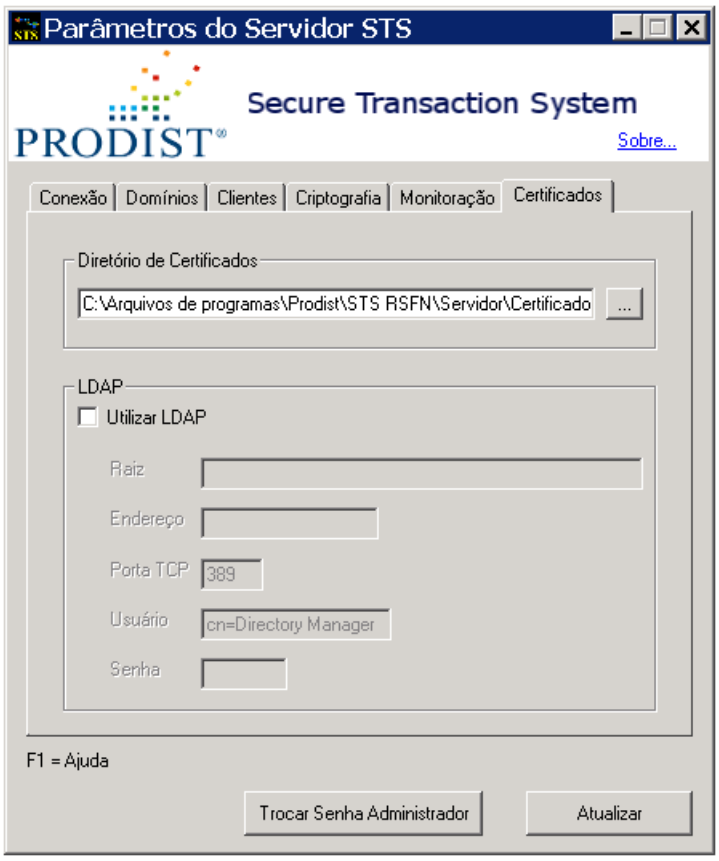
Deixe esta caixa desmarcada inicialmente. Este parâmetro será discutido mais a frente neste manual.

5.2.5 Aba <Criptografia>



Esta aba não deve ser configurada se você estiver configurando o Servidor STS pela primeira vez, a configuração dos parâmetros desta será abordada no tópico **5.5 "Configurando um servidor para utilizar o HSM".**

5.2.6 Aba <Certificados>



- Caixa **Diretório de certificados:** Este campo deverá ser preenchido com o nome da pasta raiz onde os arquivos de certificados (de sufixo **“.cer”**) serão criados e armazenados. Se você pretende que a pasta esteja alocada em algum outro ponto da rede, lembre-se que deverá utilizar uma notação do tipo UNC. Por exemplo: **“\\servidor\certificados”.** Nestes casos, o serviço **<STSServer RSFN>** não poderá ser executado sob o usuário **SISTEMA** (**SYSTEM**), que é o usuário de execução da instalação padrão. Será preciso alterar as configurações de execução do serviço, de forma que as credenciais de (logon) execução sejam credenciais de usuário local ou do domínio, com permissão de escrita e leitura no diretório informado, maiores informações de como realizar essa alteração são encontradas no **Apêndice D - Alterando a configurações de execução do serviço STS RSFN**.

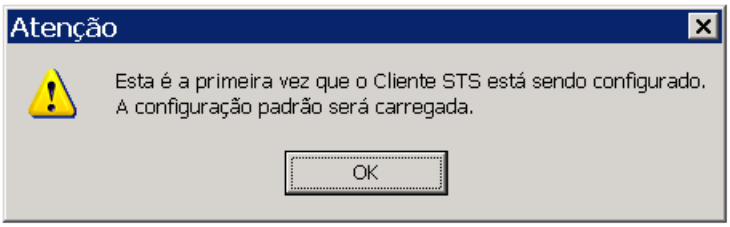
- Quadro **LDAP**: Essa opção não deve ser utilizada a partir desta versão do STS RSFN.

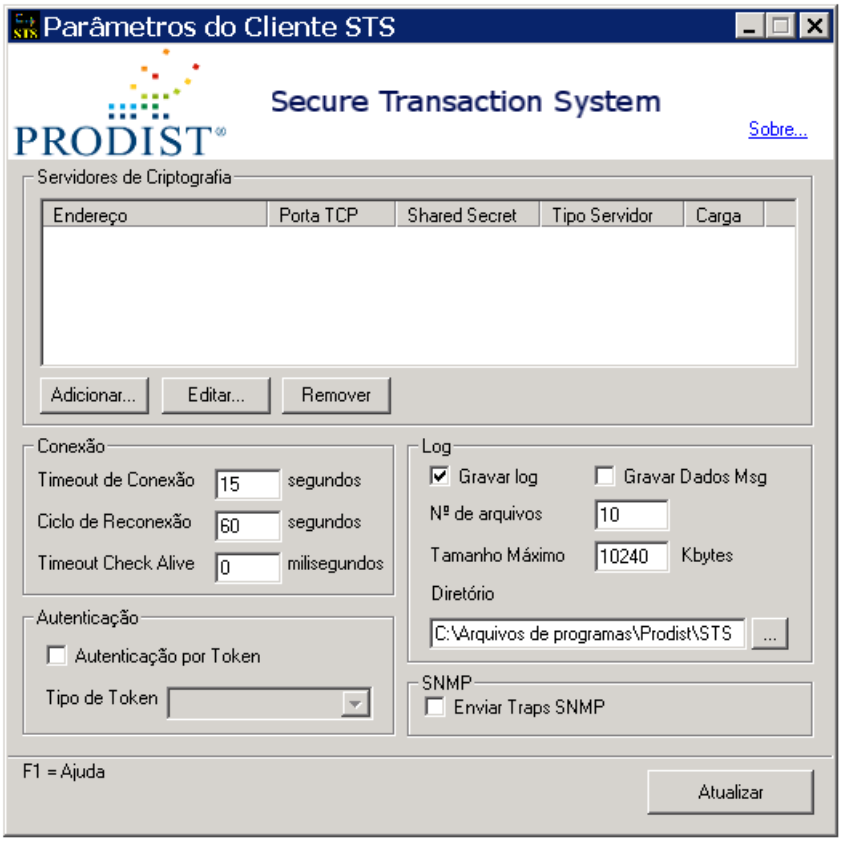
Obs.: Clique no botão **Atualizar** para gravar os dados e reiniciar o **Servidor STS,** sempre que houver uma atualização de qualquer parâmetro.

5.3 CONFIGURANDO O CLIENTE STS PARA SISTEMA WINDOWS

Execute o aplicativo de configuração do **Cliente STS**, clicando em **`Iniciar > Todos os Programas > Prodist > STS RSFN > Cliente > Parâmetros do Cliente STS.`**

Na primeira execução deste aplicativo irá aparecer uma mensagem informando que esta é a primeira vez que ele é executado. Clique no botão **[OK]** e o aplicativo de configuração será iniciado com os valores padrão.





Ao ser exibida a janela de configuração, altere o valor dos parâmetros de configuração do **Cliente STS**, de acordo com as necessidades de seu ambiente. Em um primeiro momento as caixas **"Autenticação por Token"** e **"Enviar Traps SNMP"** deverão permanecer desabilitadas. Uma breve descrição de cada campo da janela de configuração está apresentada a seguir:

- Parâmetro "**Timeout de Conexão**": Este campo deverá ser preenchido com o tempo máximo em segundos que o **Cliente STS/Thread** possui para estabelecer a conexão com o **Servidor STS**. Os valores possíveis para o campo estão na faixa de 1 a 3600 segundos.

ATENÇÃO: Ao solicitar a abertura de várias conexões simultâneas, especialmente quando cliente e servidor estiverem em redes distintas (ou se houver a presença de muito cascateamento de switch, routers, firewalls...), este campo deve receber uma maior atenção, pois o processo de estabelecer as primeiras conexões podem afetar as demais.

- Parâmetro "**Ciclo de Reconexão**": Este campo deverá ser preenchido com o intervalo de tempo entre duas verificações do status da conexão de cada ***thread*** cliente com o(s) Servidor(es) STS. No **Cliente STS** existe uma ***thread*** responsável pela monitoração e manutenção da conectividade entre todas as *threads* cliente e o(s) Servidor(es) STS disponíveis. Essa ***thread*** é necessária porque pode haver uma falha na comunicação com o servidor e, neste caso, a conexão precisará ser restabelecida.

OBS: A cada ciclo essa ***thread*** verifica o status de cada conexão *TCP socket* e, se for necessário, tenta refazer a conexão. De preferência este campo deve ter um valor de, no mínimo 15 segundos **maior** que o parâmetro "**Timeout de Conexão**"**.**

- Parâmetro "**Timeout Check Alive**": Este campo deverá ser preenchido com o tempo máximo (em milissegundos) de espera pela resposta do teste de conectividade (ICMP PING) realizado antes do envio dos pacotes de criptografia/decriptografia. É preciso ter cuidado com o uso de valores muito baixos neste parâmetro porque, caso o sistema esteja processando uma carga elevada, a resposta de cada verificação poderá demorar mais a acontecer.

Caso o tempo de ***"timeout"*** seja atingido, o Cliente STS irá, unilateralmente, fechar a conexão corrente. Isso poderá, em determinados casos, causar um erro de criptografia em conexões que não apresentavam nenhum problema.

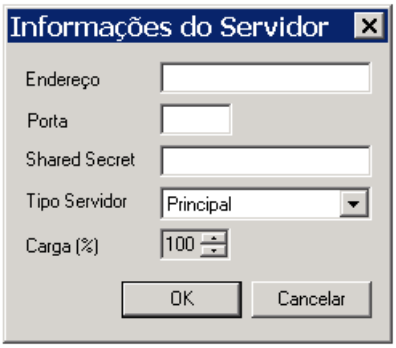
O valor padrão (default) deste parâmetro é "0" (zero), o que serve para a maioria dos ambientes de processamento e significa que o teste não será realizado.

A configuração de um valor diferente de "0" (zero) só é recomendada para ambientes com alto volume de transações concorrentes (muitas ***threads*** abertas). Recomendamos que, quando utilizado, o valor deste parâmetro seja sempre maior do que 2000 milissegundos.

- Lista "**Servidores de Criptografia**": Esta lista deverá ser preenchida com as informações para a conexão com o(s) Servidor(es) STS. É possível cadastrar vários

servidores de criptografia para um mesmo cliente. Servidores adicionais podem atuar no modo *Load Balance* ou apenas no modo *Failover*.

Deve existir, no mínimo, um servidor principal. Para adicionar um Servidor de Criptografia clique no botão **[Adicionar]** e a seguinte caixa de diálogo será exibida:



- Parâmetro **"Endereço IP"**: Este parâmetro deverá ser preenchido com o endereço IP, UNC ou Alias DNS da máquina onde está instalado o **Servidor STS**.
- Parâmetro **"Porta"**: Este parâmetro deverá ser preenchido com o número da porta TCP a ser utilizada para a conexão entre o **Servidor STS** e o **Cliente STS**. Esta porta deverá ser a mesma configurada para o **Servidor STS** no item 5.2.1 deste manual.
- Parâmetro **"Shared Secret"**: Este parâmetro deve ser preenchido com a senha (de no mínimo 8 e no máximo 36 caracteres) que tem por objetivo autenticar a conexão *TCP Sockets* entre o **Cliente STS** e o **Servidor STS**. Deve ser a mesma senha configurada na instalação do **Servidor STS**, como visto anteriormente no item 5.2.1 deste manual. Caso as senhas não sejam iguais, o **Servidor STS** não aceitará a conexão proveniente deste cliente.
- Parâmetro **"Tipo Servidor"**: Este parâmetro deve ser preenchido com o tipo de **Servidor STS** que está sendo acrescentado na configuração. Existem dois tipos possíveis:
  - **Principal** – O **Servidor STS** que será sempre utilizado. Se houver mais de um servidor configurado como principal, a carga total de processamento será distribuída entre eles, de acordo com o percentual que for estipulado para cada um, no parâmetro "**Carga**".
  - **Failover** - O **Servidor STS** é um backup que somente será acessado em caso de falha do(s) servidor(es) principal(is).
- Parâmetro "**Carga**": Este parâmetro deverá ser preenchido com o percentual de carga ao qual o servidor principal será submetido. A soma das cargas de todos os servidores principais não poderá ultrapassar os 100%.

OBS: Para editar os dados de um Servidor, selecione-o na lista e clique no botão **[Editar]**. Para remover um Servidor da lista de servidores, selecione-o e clique no botão **[Remover]**.

- Caixa "**Gravar Log**": Esta caixa deverá ser marcada para habilitar a gravação de registros de Log pelo **Cliente STS**. Ao marcar esta caixa os parâmetros "Log: Número de arquivos", "Log: Tamanho Máximo" e "Log: Diretório" serão habilitados.
- Parâmetro "**Log: N^0 de arquivos**": Este parâmetro deverá ser preenchido com o número máximo de arquivos de LOG que poderão ser criados na pasta **"\Prodist\STS RSFN\Cliente\LOG"**. No mínimo deverá haver 1 e no máximo 100 arquivos.
- Parâmetro "**Log: Tamanho máximo**": Este parâmetro deverá ser preenchido com o tamanho máximo dos arquivos de LOG em Kbytes. A faixa de valores permitida varia de `512 a 51200 Kbytes`.

Atenção: Caso o tamanho de um pacote recebido seja superior ao tamanho máximo do arquivo de LOG, o tamanho máximo do arquivo passará a ser igual ao tamanho do pacote, ignorando-se o valor configurado. Isso ocorre para que o pacote não seja partido, no momento em que o registro do evento for gerado.

- Parâmetro "**Log: Diretório**": Este parâmetro deverá ser preenchido com a pasta onde os arquivos de Log serão criados. À direita do parâmetro existe um botão para navegar pelas pastas. Se você pretende que a pasta esteja alocada em algum outro ponto da rede, lembre-se que deverá utilizar uma notação do tipo UNC. Por exemplo: **"\\servidor\certificados".** Nestes casos, o serviço **<STSClient RSFN>** não poderá ser executado sob o usuário **SISTEMA** (**SYSTEM**), que é o usuário de execução da instalação padrão. Será preciso alterar as configurações de execução do serviço, de forma que as credenciais de (logon) execução sejam credenciais de usuário local ou do domínio, com permissão de escrita e leitura no diretório informado, maiores informações de como realizar essa alteração são encontradas no **Apêndice D - Alterando a configurações de execução do serviço STS RSFN**.
- Clique no botão **[Atualizar]** para gravar os novos dados.

5.4 O CLIENTE STS JAVA

Esta aplicação tem função análoga ao Cliente Windows, mas pode ser executado sob qualquer Sistema Operacional que suporte a execução do SUN JAVA J2SE 5 ou superior. Ele é

o componente responsável pela conexão e gerência de pacotes enviados ao(s) Servidor(es) STS para geração ou abertura de pacotes padrão RSFN.

5.4.1 Configuração

O cliente Java necessita consultar um arquivo de configuração **{politicamsg.xml}**, a fim de obter as informações necessárias para efetuar a conexão com o servidor de criptografia. Esse arquivo deve ser gerado em ambiente Windows, a partir do aplicativo **<Parâmetros do Cliente>** e deve ser copiado para a máquina e pasta onde será usado o **Cliente STS Java**. As informações de registros de eventos (pasta de log, tamanho máximo do arquivo e número máximo de arquivos de log) são passadas como parâmetros do método de conexão. O **Cliente STS Java** possui um esquema de log rotativo, apagando os arquivos mais antigos, de acordo com as informações fornecidas nos parâmetros deste método.

5.4.2 Pré-requisitos

Pacote SUN JAVA J2SE 5 ou superior.

Para a configuração serão necessários os seguintes arquivos:

- Pacote **{STSClient.jar}** que é a própria aplicação Cliente JAVA e é instalada junto com a aplicação Cliente Windows.

- Após configurar o **Cliente STS Windows,** como descrito anteriormente, deve-se localizar o arquivo **{politicamsg.xml}**, que poderá ser encontrado na pasta "Cliente" da pasta de instalação do STS (por padrão, **"\Prodist\STS RSFN\Cliente"**), e copiá-lo para a máquina e pasta onde o **{STSClient.jar}** será executado.

5.4.3 Teste

Para efeito de testes, de ambiente ou de carga, a aplicação disponibiliza uma classe (classe padrão) para ser executada via linha de comando. Para utilizar a classe de testes, além dos arquivos descritos no item pré-requisitos, é preciso ter o ambiente do **Servidor STS** configurado e operacional.

A chamada para execução da classe padrão (default) de testes é:

```
java -jar STSClient.jar politicamsg.xml arquivo ISPBO ISPBD DOM S R I O T [log]
```

Onde:

- **politicamsg.xml** = caminho para o arquivo **{politicamsg.xml}**

- **arquivo** = Caminho para o arquivo a ser utilizado como ENTRADA

- **ISPBO** = ISPB da instituição de origem

- **ISPBD** = ISPB da instituição de destino

- **DOM** = Domínio de operação com 5 caracteres (STR00, MES00, DDA00, CCC00, etc.)

- **S** = Quantidade de conexões simultâneas (threads executando em paralelo)

- **R** = Quantidade de repetições da operação (**O**) em cada thread

- **I** = Intervalo em milissegundos (ms) entre cada operação (válido para todas as threads)

- **O** = tipo de operação a realizar no arquivo de ENTRADA (C = criptografia, D = decriptografia, A = ambas)

- **T** = Tipo de entrada (T = texto, B = binário)

- **[log]** = parâmetro opcional que indica a pasta onde os arquivos de registro de eventos (log) serão salvos. Se este parâmetro não for informado os arquivos de registros de eventos (logs) serão gravados na mesma pasta que o comando for executado.

Exemplo:

```
java -jar STSClient.jar politicamsg.xml teste.txt 11111111 22222222 MES00 1 1 0 a t c:\log
```

OBSERVAÇÃO: ***A chamada descrita acima não gera nenhum arquivo de saída. Sua função é testar a conectividade do sistema e servir como ferramenta de teste de carga. Você não deve utilizar esta chamada para executar qualquer tipo de tarefa diferente. Para utilizar as classes do pacote {STSClient.jar} para processamento batch de operações de criptografia e decriptografia, utilize as chamadas descritas no próximo item.***

5.4.4 Utilizando as classes do pacote {STSClient.jar} para implementar chamadas batch para operações de criptografia e decriptografia de arquivos

O pacote **{STSClient.Jar}** possui todas as classes necessárias para a integração de aplicativos Java com o **STS RSFN**. Duas destas classes podem ser chamadas através de "linha

de comando", de forma a permitir a implementação de procedimentos *batch* para as operações de criptografia e decriptografia.

Ao executar o comando do exemplo a seguir, o pacote irá exibir todas as suas possibilidades *batch*:

```
> java -jar STSClient.jar -h
```

ARGUMENTOS PARA STRESS TEST:
1- Path para o arquivo de politica
2- Path para o arquivo de teste
3- ISPB de Origem
4- ISPB de Destino
5- Domínio
6- Números de conexões simultâneas
7- Números de repetições
8- Intervalo de operações (ms)
9- Operação: (c)riptografia, (d)ecriptografia, (a)mbos
10- Tipo de entrada: (t)exto ou (b)inário
[11]- (Opcional) Diretório de log. Se nenhum valor for passado o log será salvo do diretório corrente.

Exemplo da chamada padrão:

```
java -jar STSClient.jar politicamsg.xml ArquivoTeste.txt 11111111 11111111 SCG00 1 1 a t c:\log
```

ARGUMENTOS PARA CRIPTOGRAFIA DE ARQUIVO (CryptFile):
1- Path para o arquivo de politica
2- ISPB de Origem
3- ISPB de Destino
4- Domínio
5- Path para o arquivo de entrada
6- Path para o arquivo de saída
7- Código da operação:
- **0 - criptografa e assina texto**
- **6 - assina texto**
- **8 - criptografa e assina binário**
- **10 – assina binário**

[8]- (Opcional) Diretório de log. Se nenhum valor for passado o log será salvo no diretório corrente.

EXEMPLO DA CHAMADA Cryptfile:

```
java -cp STSClient.jar br.com.prodist.sts.client.file.CryptFile politicamsg.xml 11111111
11111111 SCG00 ArquivoEntrada.zip ArquivoSaida.cri 8
```

ARGUMENTOS PARA DECRIPTOGRAFIA DE ARQUIVO (DecryptFile):

1- Path para o arquivo de politica
2- ISPB de Origem
3- ISPB de Destino
4- Domínio
5- Path para o arquivo de entrada
6- Path para o arquivo de saída
[7]- (Opcional) Diretório de log. Se nenhum valor for passado o log será salvo no diretório corrente.

EXEMPLO DA CHAMADA DecryptFile:

```
java -cp STSClient.jar br.com.prodist.sts.client.file.DecryptFile politicamsg.xml 11111111
11111111 SCG00 ArquivoEntrada.cri ArquivoSaida.zip
```

Utilize as classes:

- `br.com.prodist.sts.client.file.CryptFile`
- `br.com.prodist.sts.client.file.DecryptFile`

Para criptografar e decriptografar arquivos na modalidade batch (linha de comando).

5.4.5 Utilizando as classes do pacote {STSClient.jar} para realizar chamadas *batch* para operação da Atualização de Certificado

A chamada é muito parecida com as operações de criptografar e decriptografar, porém com uma alteração na utilização da classe:

ARGUMENTOS PARA ATUALIZAÇÃO DE CERTIFICADO (UpdateCertificate):
1- Path para o arquivo de politica
2- ISPB de Origem
3- ISPB de Destino
4- Domínio
5- Path para o arquivo do certificado

EXEMPLO DA CHAMADA UpdateCertificate:

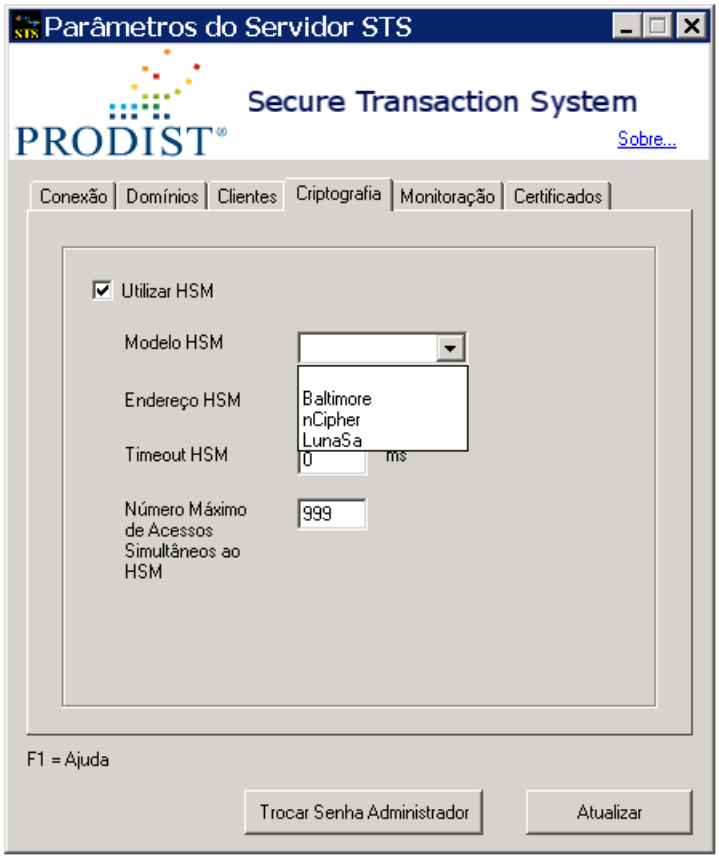
```
java -cp STSClient.jar br.com.prodist.sts.client.file.UpdateCertificate politicamsg.xml
11111111 11111111 SCG00 ArquivoCertificado.cer
```

5.5 CONFIGURANDO O SERVIDOR STS PARA UTILIZAR UM HSM

Depois de instalado o driver do HSM a ser utilizado (Consulte o manual de instalação do HSM correspondente), o **Servidor STS** pode ser configurado para utilizá-lo.

Execute o aplicativo de configuração de **<Parâmetros do Servidor STS>** e clique na Aba **<Criptografia>**.

Marque a caixa **[Utilizar HSM]** e escolha qual o tipo de HSM será utilizado, na caixa **[Tipo de HSM]**. As opções possíveis estão listadas de acordo com os fabricantes ou modelos dos HSM (Baltimore, nCipher, Luna SA).



- Campo **"Endereço HSM"** – refere-se ao endereço IP do HSM que será utilizado. ***Se você estiver utilizando mais de um HSM em esquema de Load Balance, tratado pelo próprio driver dos HSM***, você deve utilizar o valor **`0.0.0.0`.**

- Campo "**Timeout HSM**" – refere-se ao tempo máximo que o **Servidor STS** vai aguardar pela resposta ao teste de validação da conexão com o HSM. O servidor verifica se o HSM está ativo e apto a responder as requisições do **Servidor STS**, antes de enviar qualquer solicitação. Antes de aceitar o pedido de conexão de um novo

Cliente STS ou de enviar um pedido de criptografia de um **Cliente STS** já conectado, o **Servidor STS** testará a disponibilidade do HSM. Se depois de decorrido o tempo especificado por este parâmetro o HSM não responder, um evento de erro de comunicação com o HSM será gerado e o **Servidor STS** não irá mais aceitar conexões de qualquer **Cliente STS**, até que ele detecte que a conexão com o HSM foi restabelecida.

Este parâmetro deverá ser preenchido com o valor máximo de tempo de espera admissível pela resposta do HSM.

Se este parâmetro for preenchido com o valor “0” (zero) o teste não é efetuado.

Este parâmetro está diretamente relacionado com a detecção de erros na comunicação entre o **Servidor STS** e o **HSM**.

Observações:

Caso o valor deste parâmetro esteja muito baixo e a carga de processamento esteja muito alta, o HSM pode demorar a responder ao teste e isso causará erro (falso positivo) no **Servidor STS**. Isso provocará uma degradação no desempenho do ambiente como um todo.

Por outro lado, caso o valor esteja muito alto, o servidor irá levar mais tempo para detectar e acusar possíveis erros e continuará aceitando requisições dos **Clientes STS**, que irão falhar e, consequentemente, demorará mais para adotar os procedimentos de recuperação de falhas.

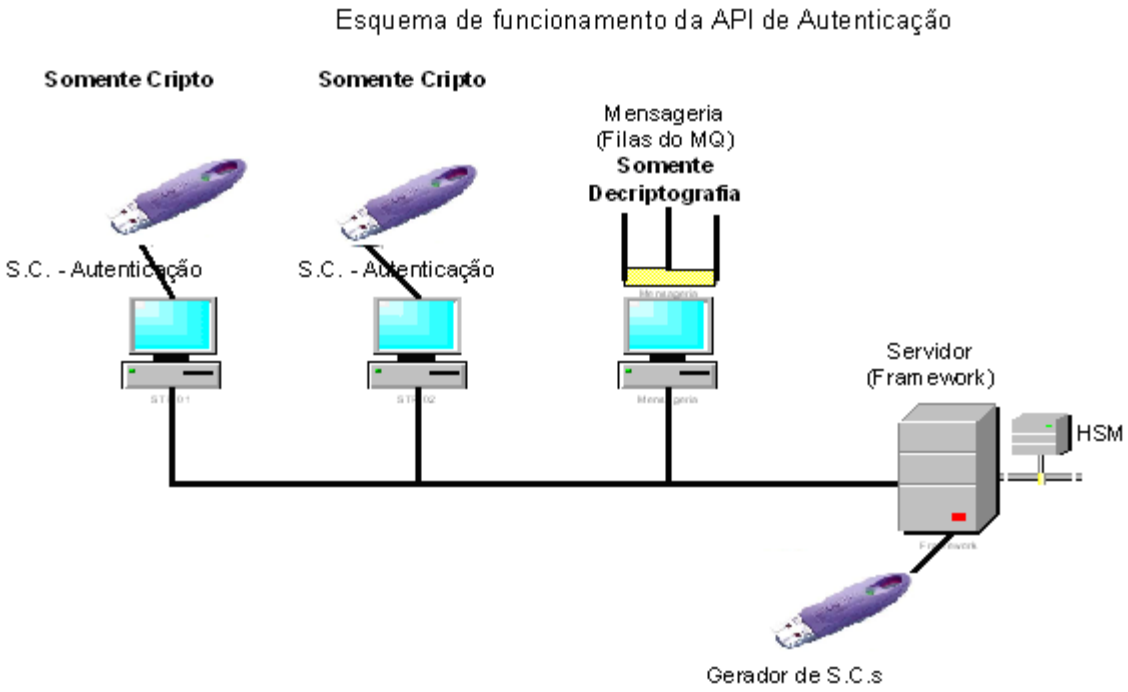
Nota: É importante ainda ressaltar que se a carga de requisições for muito alta, o valor deste campo for “0” (zero) e ocorrer erro na conexão com o HSM, pode ser que o **Servidor STS** nem volte a aceitar conexões.

Obs.: Para a grande maioria dos ambientes o valor recomendado é “0” (zero), o que significa que o teste não será realizado.

Configure valores diferentes de “0” (zero) neste parâmetro, apenas se o seu ambiente processar um número de transações concorrentes muito elevado, ou se houver recomendação da equipe de suporte da PRODIST.

5.6 ESQUEMA DE AUTENTICAÇÃO POR TOKEN

O STS é dotado de um esquema de autenticação (opcional) por Token Criptográfico entre o cliente e servidor.



Este esquema é opcional e <u>pode</u> ser contratado a parte, mas só está disponível para Clientes Windows e para ambientes que utilizem HSM. Ele fornece funcionalidades para autenticação forte dos usuários que utilizarão o **Servidor STS** e implementa a criptografia nos pacotes de dados que trafegam entre o cliente (Mensageria) e o servidor da aplicação. Este esquema de autenticação utiliza Tokens ikey 2032 da Safenet.

O primeiro passo na configuração deste esquema é a configuração dos Tokens nas máquinas que utilizarão o sistema de criptografia e na máquina onde o **Servidor STS** está instalado. Este sistema de autenticação é baseado na geração de pares de chaves que estarão armazenados nos HSM da solução, por isto é indispensável à prévia instalação e configuração do HSM.

Instale o driver do Token nas máquinas (cliente e servidor) que participarão do esquema de autenticação.

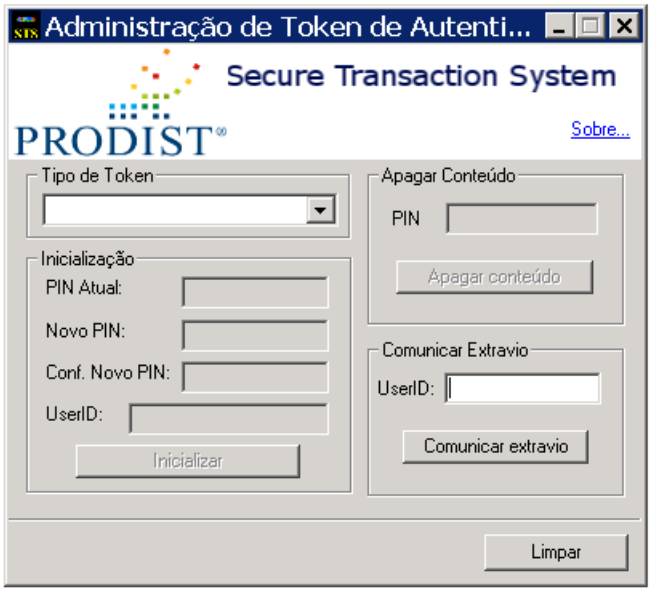
Após a instalação do driver do Token, formate cada um deles, com a aplicação da própria Safenet, e associe um PIN (senha) padrão, que posteriormente deverá ser trocado pelo usuário.

O administrador deverá utilizar o aplicativo de **<Administração do Token>** para inicializar os Tokens no sistema STS e configurar o ambiente em que eles deverão ser utilizados.

5.6.1 Administração do Token (Servidor STS)

Cada Token de operador deverá ser inicializado pelo administrador do sistema antes que possa ser utilizado para autenticação no sistema STS.

Esta inicialização é feita com o aplicativo **<Administração do Token>**, que está disponível na máquina onde o Servidor STS foi instalado. Após clicar em **`Iniciar > Todos os Programas > Prodist > STS RSFN > Servidor > Administração do Token`** será exibida uma janela para a digitação de um PIN. Este PIN é a senha de acesso ao HSM, o mesmo que é usado na janela do aplicativo de **<Administração de Chaves Privadas>** para expandir a árvore de chaves do HSM. Se o PIN estiver correto, a seguinte janela será exibida:



Esta janela possui três seções distintas, uma para a inicialização do Token e alteração do PIN (senha), outra para apagar o conteúdo de um Token e uma terceira para comunicar o extravio de um Token. Iremos explorar melhor essas funcionalidades abaixo:

Seção Inicialização:

- Campo “**PIN Atual**”: Esse campo deve ser preenchido com o PIN atual do Token. Após a formatação do Token, pelo aplicativo da Safenet, o PIN padrão é “PASSWORD”.
- Campo **“Novo PIN**”: Esse campo deve ser preenchido com o valor do novo PIN. Preencha este campo somente se desejar alterar o PIN do Token.
- Campo “**Conf. Novo PIN**”: Esse campo é utilizado para confirmar o PIN anterior, deve ser preenchido com o mesmo valor do campo anterior. Preencha este campo somente se houver preenchido o campo “**Novo PIN**”.
- Campo “**UserID**”: Esse campo deve ser preenchido com a identificação única do usuário do Token. O tamanho máximo deste campo é 11 caracteres e sugerimos utilizar o número do CPF do usuário, de forma a identificar, inequivocamente, o dono do Token.
- Botão **[Alterar]**: Clique neste botão para proceder a inicialização do Token e a alteração de senha (se for o caso).
- Botão **[Limpar]**: Clique neste botão para apagar todos os campos da janela.

Seção Apagar Conteúdo

- Campo “**PIN**”: Deve ser preenchido com o PIN atual do Token.
- Botão **[Apagar Conteúdo]**: Clicando nesse botão o conteúdo atual do Token será apagado.

Seção Comunicar Extravio

- Campo “**UserID**”: Esse campo deve ser preenchido com a identificação do usuário do Token.
- Botão **[Comunicar Extravio]**: Clicando nesse botão, o Token associado ao **UserID** informado será invalidado no sistema. Ele não poderá mais ser utilizado no sistema STS e a chave do usuário será apagada do HSM.

5.6.2 Configuração do Token nas estações Cliente STS

Após terem sido instalados os *drivers* nas estações clientes, os usuários poderão alterar, a qualquer momento, o PIN (senha) de seus Tokens. Para isto deverão utilizar o aplicativo **<Configuração do Token>** que foi instalado juntamente com o **Cliente STS**. Para iniciar este

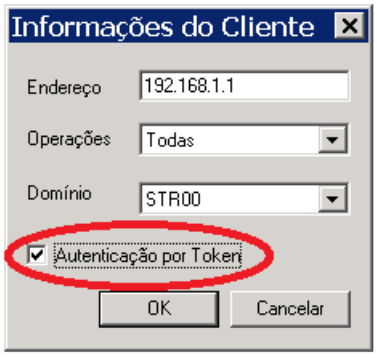
aplicativo clique em **Iniciar > Todos os Programas > Prodist > STS RSFN > Servidor > Cliente > Configuração do Token.**

A janela acima será exibida e os campos e controles são:

- Campo "**PIN Atual**": Esse campo deve ser preenchido com a senha atual do Token.
- Campo "**Novo PIN**": Esse campo deve ser preenchido com o valor da nova senha.
- Campo "**Conf. Novo PIN**": Esse campo deve ser preenchido também com o valor do campo "novo PIN", para confirmá-lo.
- Campo "**UserID**": Esse campo deve ser preenchido com a identificação do usuário do Token.
- Botão **[Alterar]**: Clique neste botão para alterar o PIN do Token.

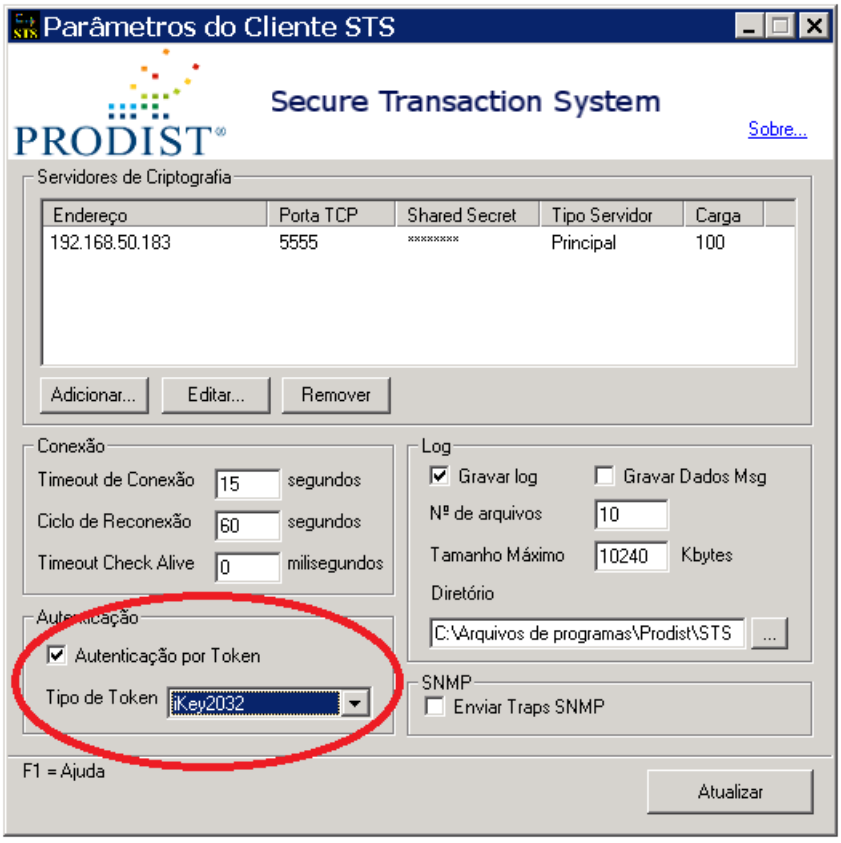
5.6.3 Habilitando a autenticação por Token no Servidor STS

Após a geração dos Tokens dos usuários, é necessário configurar o(s) Servidor(es) STS para utilizar o esquema de autenticação por Tokens. Para isto, execute o aplicativo **<Parâmetros do Servidor STS>** e edite cada um dos **clientes autorizados** que deverão utilizar Token. Ao ser exibida a janela de **<Informações do Cliente>** marque a caixa **[Autenticação por Token]**. Em seguida, clique em **[OK]** para gravar os parâmetros alterados e clique em **[Atualizar]** para reiniciar o serviço **<STSServer RSFN>**.



5.6.4 Habilitando a autenticação por Token no Cliente STS

Após a geração dos Tokens dos usuários, é necessário configurar o(s) Cliente(s) STS para que possam utilizar a autenticação por Tokens. Para isto, execute o aplicativo **<Parâmetros do Cliente STS>** e marque a caixa "**Autenticação por Token**". Clique no botão **[Atualizar]** para gravar os parâmetros alterados e reinicie o serviço **"STSClient RSFN"**, utilizando a interface de gerência de serviços do Windows (**services.msc**) *através do Prompt de Comando* ou do Painel de Controle, para que as alterações surtam efeito.



5.6.5 SNMP

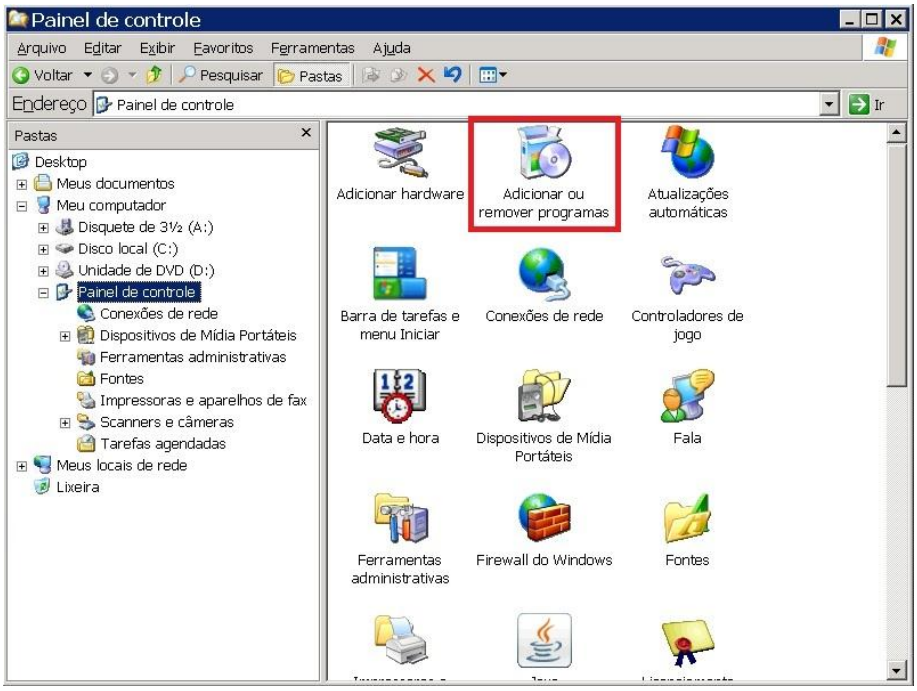
5.6.5.1 Instalação do Serviço SNMP do Windows

O STS pode gerar eventos SNMP (Simple Network Management Protocol) para facilitar a tarefa de monitoramento do estado de seus componentes.

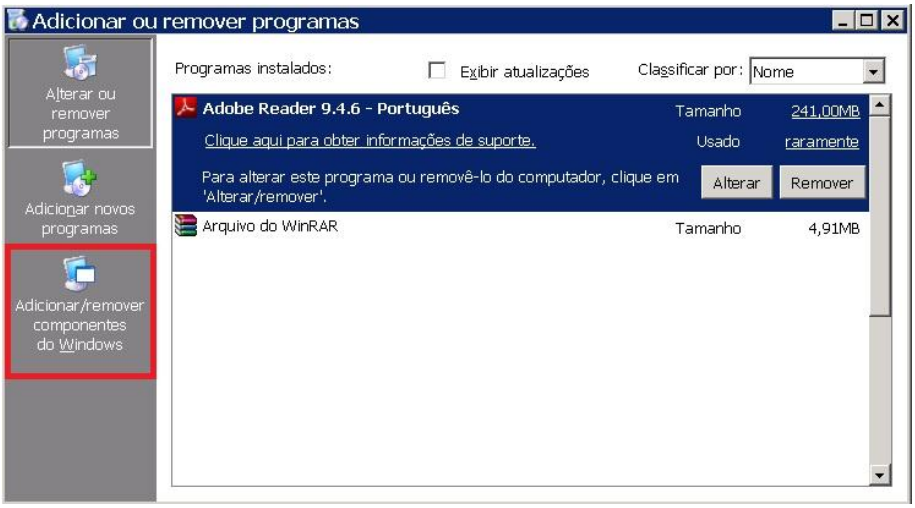
Se você deseja utilizar os recursos de geração de eventos SNMP, deve instalar o suporte a este protocolo, nas máquinas que utilizem os serviços STS (servidor e/ou cliente).

O SNMP pode ser habilitado no Windows a partir do **<Painel de Controle>.** Veremos a seguir como fazer para habilitá-lo:

a) Abra o **<Painel de Controle>** em seguida abra o **<Adicionar ou remover programas>.**

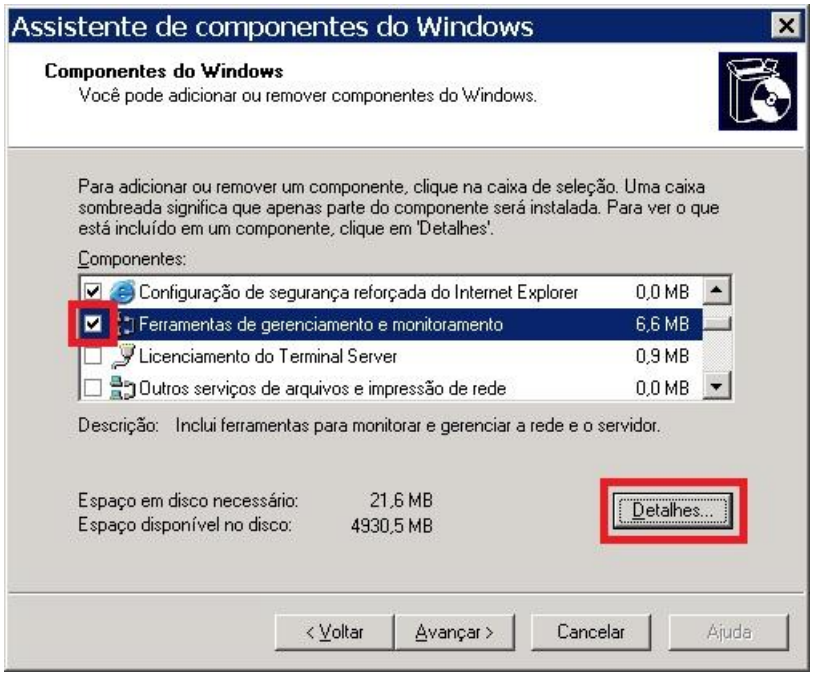


b) Clique na opção “Adicionar/remover componentes do Windows” localizada no menu à esquerda da janela.

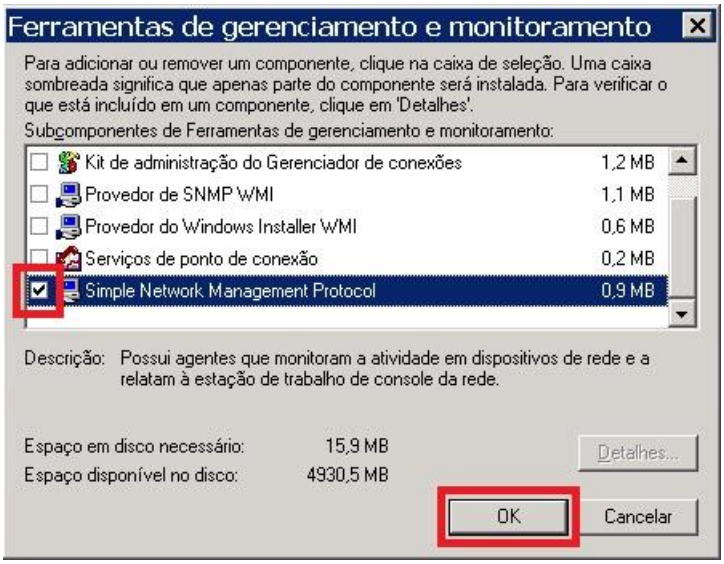


c) A tela de “Instalação do Windows” irá aparecer, aguarde até que ela termine de carregar.

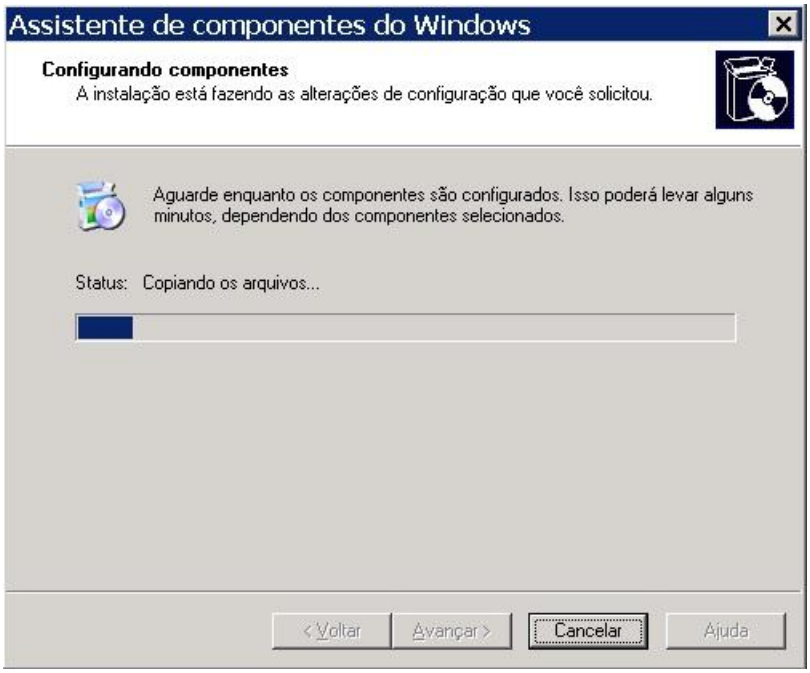
d) Quando a janela “Assistente de componentes do Windows” aparecer, selecione a opção “Ferramentas de gerenciamento e monitoramento” e clique no botão **[Detalhes]**.



e) Na janela de “Ferramentas de gerenciamento e monitoramento”, selecione a opção “Simple Network Management Protocol” e confirme clicando no botão **[OK]**.



f) Ao retornar na janela “Assistente de componentes do Windows” clique no botão **[Avançar>]** para que o protocolo SNMP seja instalado. Será necessário o CD de instalação do Windows para completar a instalação.



g) Ao finalizar de carregar a barra, clique no botão **[Concluir]** para finalizar a instalação e reinicie o computador.

5.6.5.2 Registrando as MIBs dos aplicativos do STS

Para que uma ferramenta de gerência de rede possa estar apta a receber eventos de um determinado aplicativo é necessário um prévio registro da MIB daquele aplicativo.

As MIBs dos aplicativos do STS estão nos seguintes arquivos:

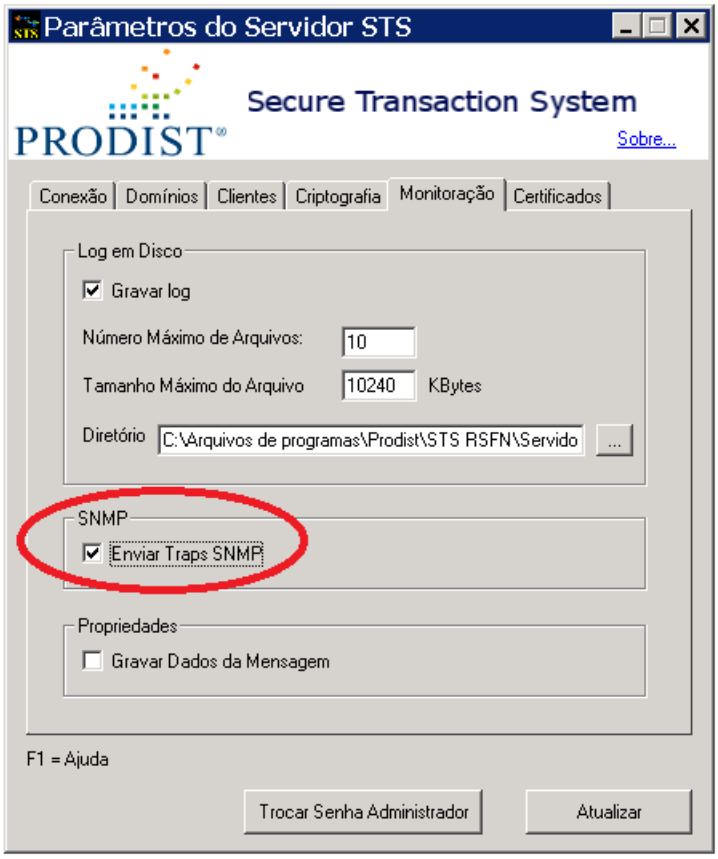
- **MIB do Serviço STS**: chama-se **{STS_Server.mib}** e está localizada na pasta **Prodist\STS RSFN\Servidor**.
- **MIB do Cliente STS**: chama-se **{STS_Client.mib}** e está localizada na pasta **Prodist\STS RSFN\Cliente**.

  Registre as MIB dos serviços do **STS**, de acordo com o manual de configuração de seu produto de gerência de eventos SNMP.

5.6.5.3 Configurando o Servidor STS para enviar eventos SNMP

Execute o aplicativo de configuração **<Parâmetros do Servidor STS>**.

a) Na aba **Monitoração** seção **SNMP**, marque a caixa "**Enviar Traps SNMP**".

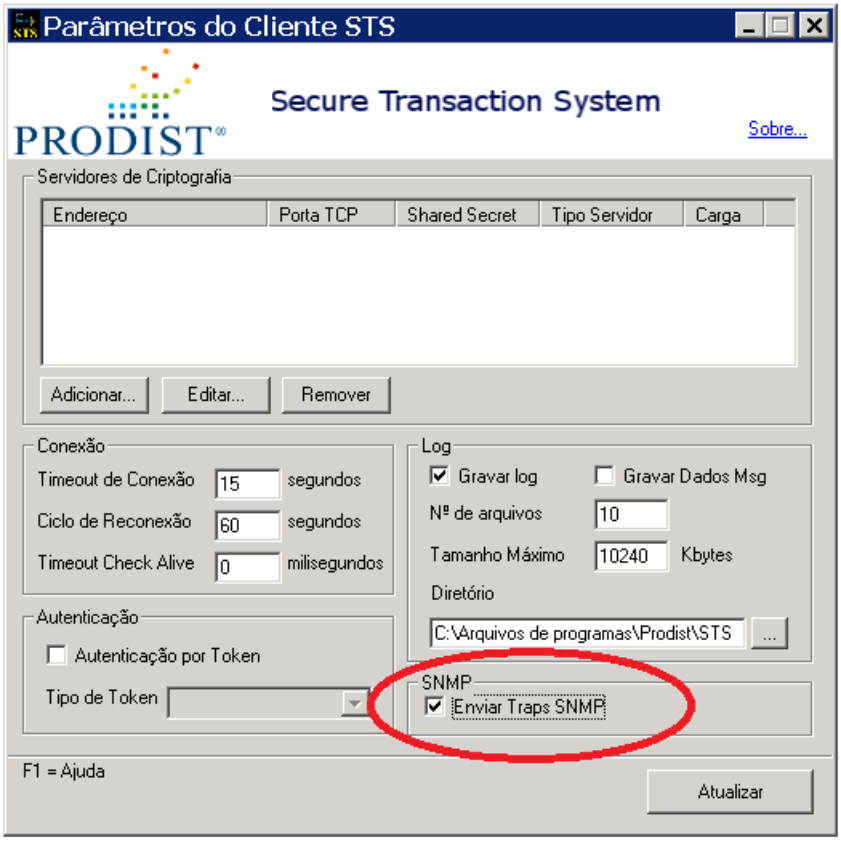


b) Clique no botão **[Atualizar]**.

5.6.5.4 Configurando o Cliente STS para enviar eventos SNMP

Execute o aplicativo de configuração **<Parâmetros do Cliente STS>**.

(a) Na seção **SNMP**, marque a caixa "**Enviar Traps SNMP**" (análogo ao procedimento feito para o Servidor STS).



(b) Clique no botão **[Atualizar]**. Será necessário reiniciar o serviço "**STSClient RSFN**".

5.7 UTILIZANDO O APLICATIVO DE ADMINISTRAÇÃO DE CHAVES PRIVADAS

O aplicativo **<Administração de Chaves Privadas>** é o responsável por todos os procedimentos de geração e gerência de pares de chaves criptográficas, CSR (Certificate Signing Request) e a exportação de certificados. Ele deve ser utilizado para gerenciar tanto chaves que estarão armazenadas em HSM quanto no Hard-Disk (HD). Para executar este aplicativo clique em **`Iniciar > Todos os Programas > Prodist > STS RSFN > Servidor > Administração de Chaves Privadas.`**

Antes de executar este aplicativo, tenha certeza de ter criado, pelo menos, um domínio através do aplicativo **<Parâmetros do Servidor>**.

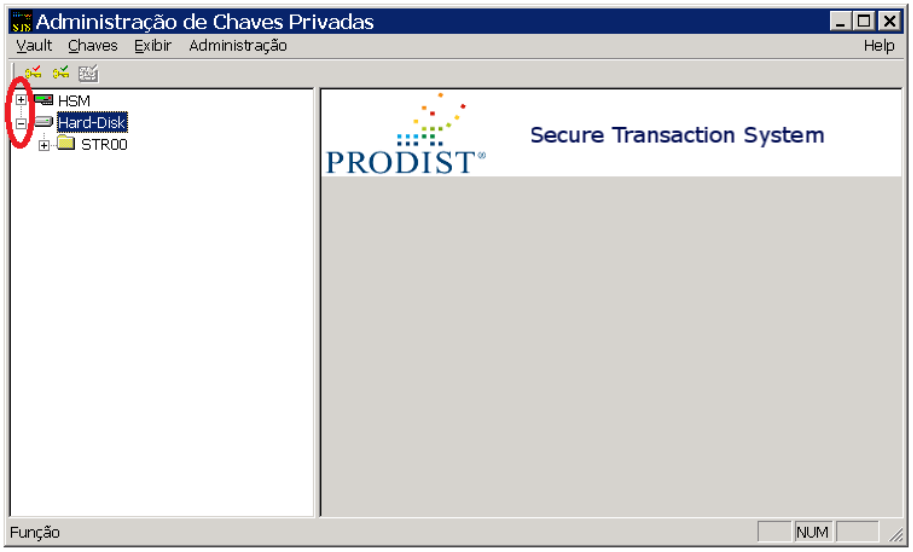
Nota: É importante lembrar que após efetuar algum procedimento relacionado com a gerência de chaves é necessário **reiniciar o STSServer RSFN.**

Para reiniciar o **Servidor STS** clique em **`Iniciar > Executar`** e digite **`"services.msc"`**.

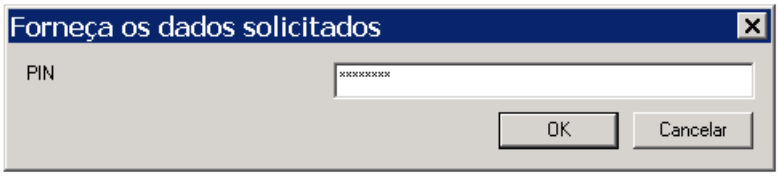
Em seguida, selecione "**STSServer RSFN**" na lista de serviços e, utilizando as opções disponíveis pelo uso do botão direito do mouse, clique nos botões **[Parar]** e depois **[Iniciar]**.

5.7.1 Gerenciando chaves privadas no HSM e no Hard-Disk

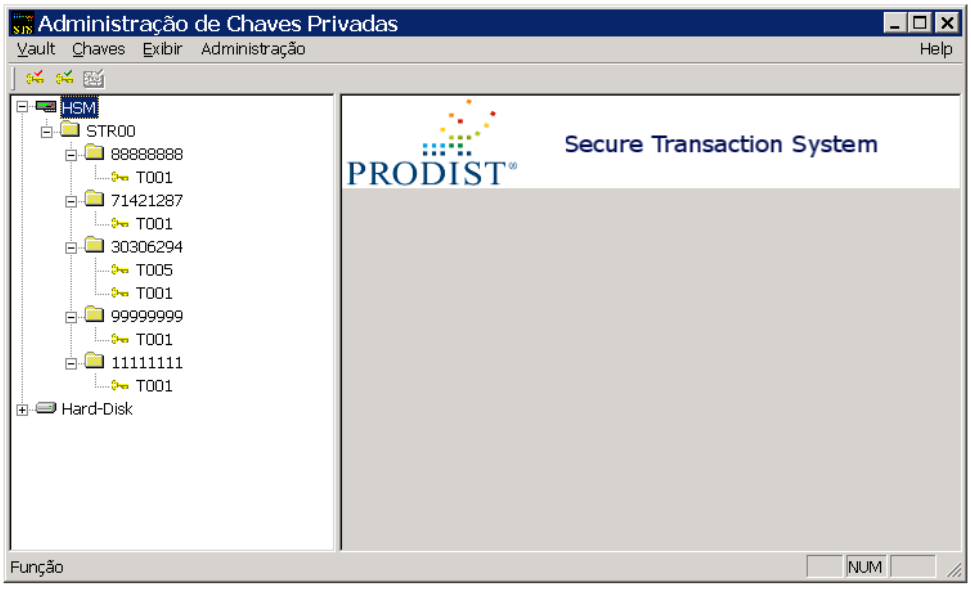
Para gerenciar as chaves privadas tanto no HSM quanto em Hard-Disk é necessário primeiro iniciar uma sessão de utilização com um desses repositórios. Para isso, clique com o botão direito sobre um dos ícones HSM ou Hard-Disk e selecione a opção "**Abrir**", ou clique no símbolo "**+**" ao lado do ícone "HSM" ou "Hard-Disk".



Se o administrador do STS abrir uma sessão com um HSM, a janela a seguir será apresentada com a solicitação do "PIN" (senha) de acesso ao HSM. Caso a opção seja o "Hard-Disk" esta janela não será exibida.

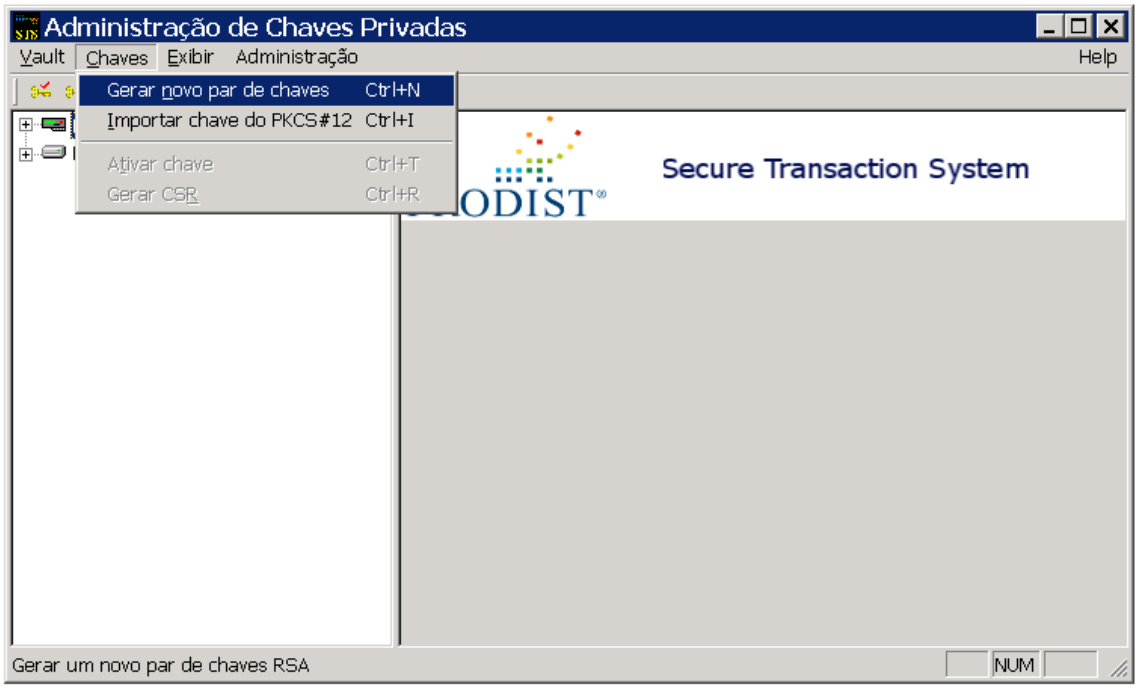


Se você digitar o PIN do HSM corretamente, as chaves existentes serão exibidas, agrupadas por ISPB conforme a imagem a seguir:

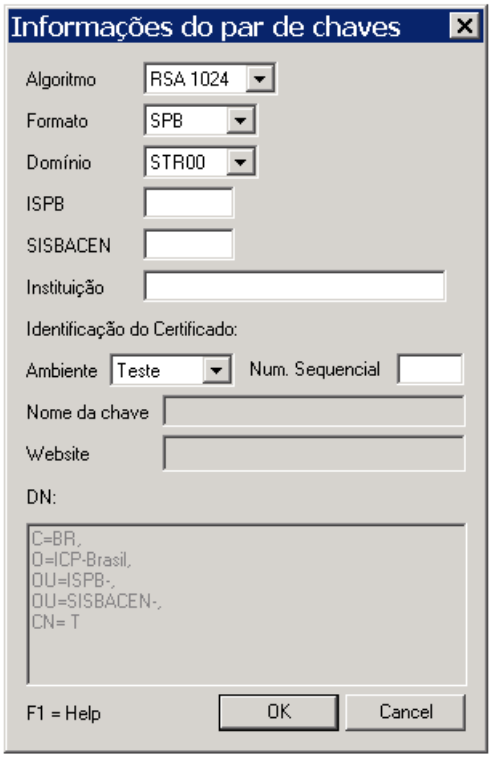


5.7.2 Criando e ativando um novo par de chaves

Para criar um novo par de chaves utilizando o aplicativo **<Administração de Chaves Privadas>**, selecione o ícone HSM ou Hard-Disk no aplicativo, clique na opção "***Chaves***" e, no menu suspenso que aparecerá, clique em "***Gerar novo par de chaves***".



A janela a seguir será exibida e você deverá preencher os dados de acordo com as especificações do manual de segurança do sistema para o qual o par de chaves estiver sendo gerado. Ex: SPB, SGC, DDA, etc.



Os campos e controles são:

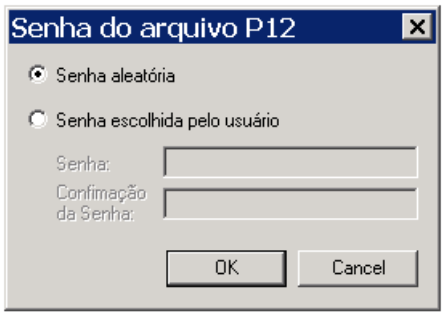
- **Algoritmo**: Especifica qual será o algoritmo do par de chaves a ser criado. As opções são: RSA 1024 ou RSA 2048. O algoritmo RSA 2048 só deve ser selecionado se você configurou o **Servidor STS** para trabalhar de acordo com a versão 2 do protocolo de segurança do BACEN. Veja o item 5.2.2 deste manual.
- **Formato**: Define o formato da DN (Distinguished Name) da chave pública. Existem alguns formatos pré-definidos e um formato livre. No formato livre é possível editar o campo DN da forma que desejar. O formato SPB é o adequado para: SPB e MES (DDA, CCS, etc.).

  Existem ainda mais 3 formatos disponíveis, a saber:
  - ✓ SCG - para o Sistema de Controle de Garantias operado pela CIP.
  - ✓ C3 - para o Sistema de Central de Cessões de Crédito operado pela CIP.
  - ✓ Livre - para qualquer outro sistema.
- **Domínio**: Domínio sob o qual do par de chaves deverá ser criado.
- **ISPB**: ISPB da instituição financeira, geralmente definido pelos oito primeiros dígitos do CNPJ da instituição. É o código da instituição proprietária do par de chaves.
- **SISBACEN**: Outro campo de controle definido pelo BACEN. Este campo só estará disponível se o formato escolhido for SPB.
- **Instituição**: Razão social da instituição financeira.
- **Identificação do Certificado**:

- **Ambiente**: a opção **Teste** serve para criar par de chaves de homologação, testes ou desenvolvimento. A opção **Produção** serve para criar par de chaves de produção.
- **Num. Sequencial**: Número sequencial de identificação das chaves, sempre criado com três algarismos.

- **Nome da Chave**: o nome da chave é gerado automaticamente quando os dados de ambiente e número sequencial são preenchidos.
- **Website**: o host e o domínio da instituição. Pode-se utilizar um host fictício com o domínio da instituição, esta opção só é habilitada em chaves nos formatos SCG e C3.

Adicionalmente, se você estiver criando um par de chaves em "Hard-Disk", a aplicação irá solicitar que você informe uma senha para a chave privada, através da seguinte janela:



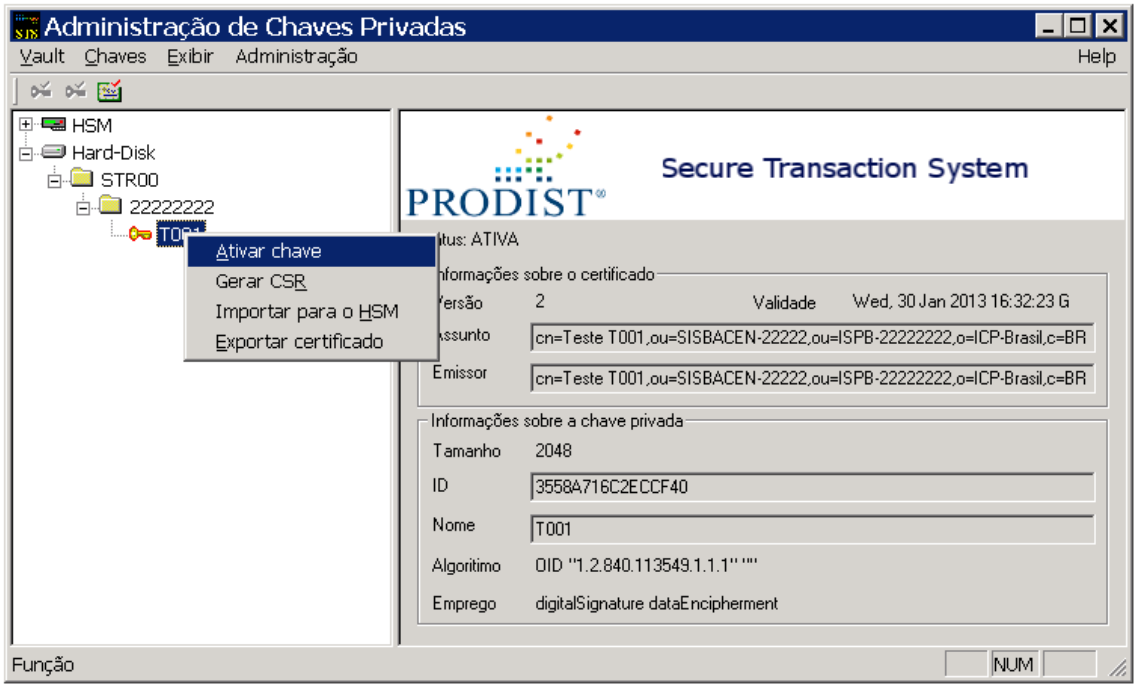
A senha pode ser aleatória ou informada pelo usuário (mínimo de 8 e máximo de 128 caracteres).

A senha aleatória pode ser recomendada para a geração de par de chaves de produção, pois é a opção que confere o maior grau de proteção a um arquivo do tipo PKCS#12 (`.p12`). Entretanto, como **nunca mais** será possível ter acesso a esta senha, **este arquivo ".p12" só poderá ser utilizado pelo aplicativo STS e as chaves jamais poderão ser importadas para qualquer outra aplicação ou HSM**. Neste caso, após a criação do par de chaves é fundamental fazer um backup do arquivo **`{vault.sts}`** e do arquivo com sufixo **`".p12"`**, mantendo-se ainda uma cópia de segurança do arquivo **{seed.p8}**, gerado na instalação do produto.

A opção de senha informada pelo usuário é a recomendada para os pares de chaves criados para fins de teste, para chaves que necessitem ser utilizadas por outras aplicações, ou ainda, para chaves que deverão ser importadas futuramente para HSM. Se esta for a opção escolhida para proteção de chaves de produção, recomendamos utilizar um esquema de, no mínimo, "**dupla custódia**" da senha. Ou seja, dividir a senha em duas partes e cada parte ser de conhecimento de um usuário diferente.

Caso a criação do par de chaves tenha sido realizada com sucesso, antes que a chave privada esteja apta para o uso, é necessário ativá-la. Para isso, clique com o botão direito do

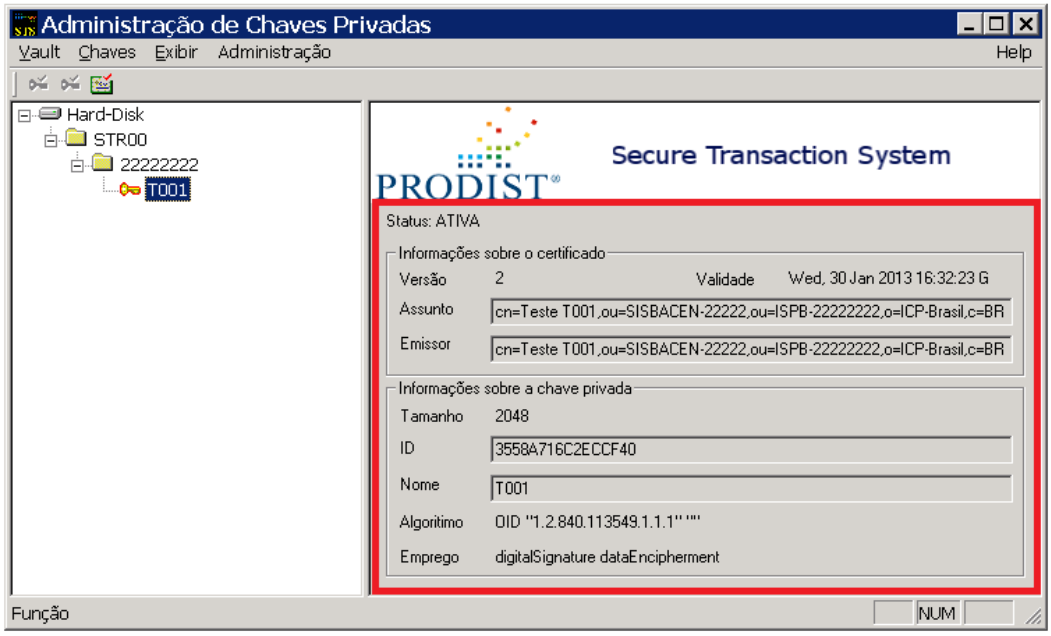
mouse sobre a chave em questão selecione a opção **"Ativar chave".** Após este procedimento, a chave passará a ser representada na janela com um contorno em vermelho ( ).



Embora uma mesma cópia do STS possa ser utilizada para assinar pacotes RSFN para mais de um ISPB (instituição independente), somente poderá existir uma chave ativa, por ISPB/Domínio. Isso significa que cada instituição, representada por seu respectivo ISPB, só pode ter uma chave ativa por domínio (STR00, MES00, DDA00...).

ATENÇÃO: Se você estiver ativando uma chave para um conjunto ISPB/Domínio que já possua uma chave ativa, a chave que estava ativa anteriormente será **desativada**.

Para verificar os dados da chave, clique no ícone da chave e seus dados poderão ser verificados no quadro que será apresentado ao lado.



IMPORTANTE: Após a criação de chaves privadas é fundamental a realização de um backup destas chaves e dos arquivos a ela relacionados. Veja a seguir quais são os arquivos/pastas que devem ser copiados, de acordo com o dispositivo de armazenamento de chaves que estiver sendo utilizado:

RELAÇÃO DE ITENS QUE DEVEM SER COPIADOS APÓS A CRIAÇÃO DE CHAVES PRIVADAS

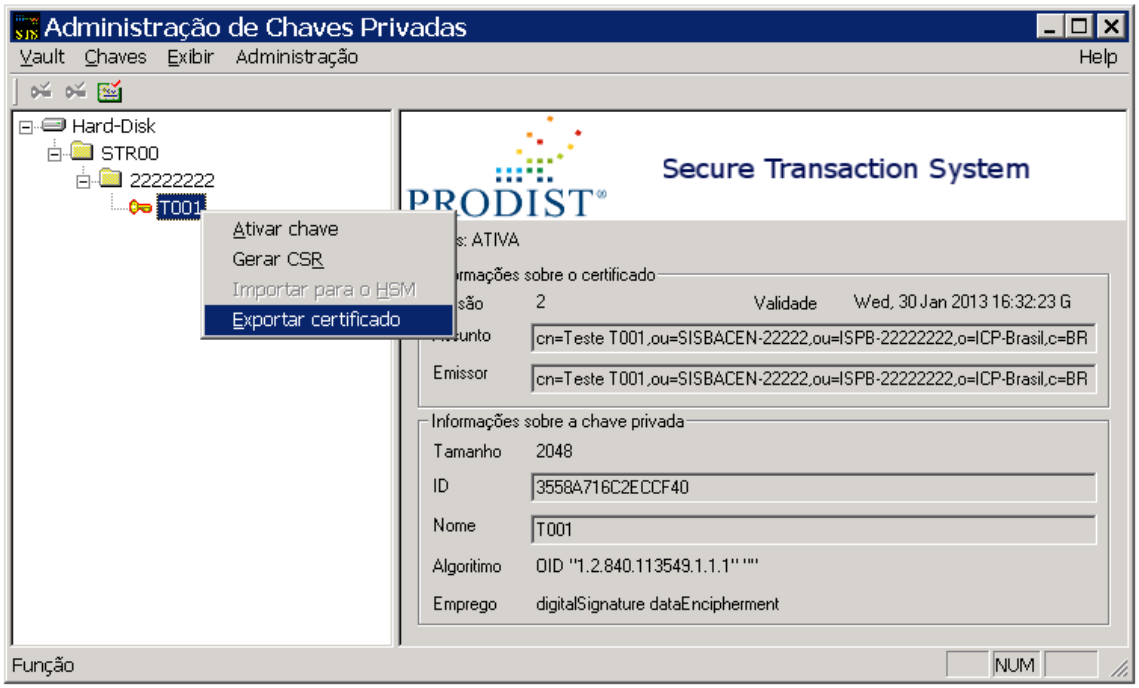
HSM nCipher nFast	Os seguintes backups são necessários: ▪ Pasta **\nFast\Kmdata\local** ▪ Arquivo **vault.sts** ▪ Smartcards com chaves de aplicação
Safenet LunaSA	Os seguintes backups são necessários: ▪ Arquivo **vault.sts** ▪ Token (PCMCIA) contendo o backup das chaves ▪ Chaves do KEY PED (se utilizado)
Hard-Disk	Os seguintes backups são necessários: ▪ Arquivo **vault.sts** ▪ Arquivos ***".p12"** existentes na subpasta **\Servidor\Vault**, da pasta de instalação do produto.

5.7.3 Geração de certificado '*FAKE*' para testes e homologação

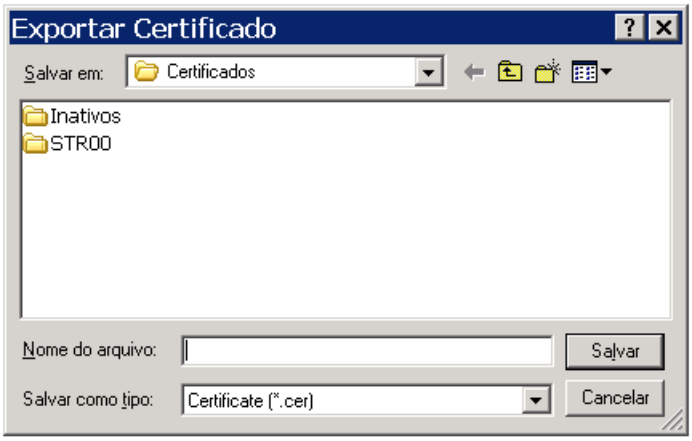
Embora geralmente os sistemas financeiros exijam o uso de certificados ICP-Brasil em seus ambientes (Homologação e Produção), você pode querer emitir certificados auto-assinados para ambientes de teste. Este tipo de certificado, conhecido vulgarmente como '***FAKE***', pode ser gerado pelo aplicativo **<Administração de Chaves Privadas>.**

Para criar um certificado auto-assinado, execute o aplicativo **<Administração de Chaves Privadas>** e identifique a chave privada para a qual você deseja emitir o certificado '***FAKE'***.

Clique com o botão direito do mouse sobre a chave e escolha a opção "**Exportar certificado"**.

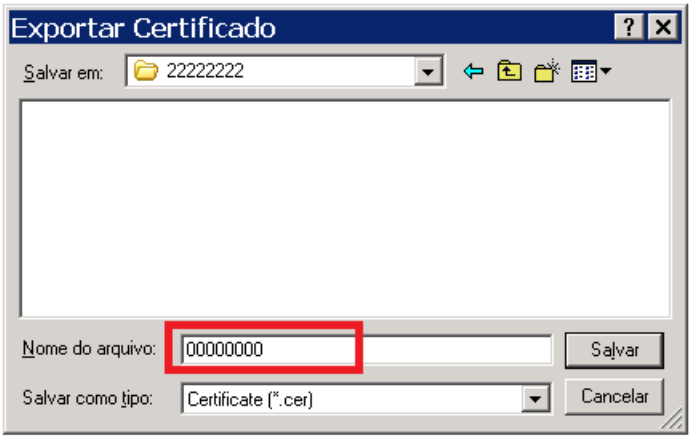


A janela **"Exportar Certificado"** será exibida. Selecione a pasta que identifica o domínio proprietário da chave em questão e clique duas vezes sobre ela.



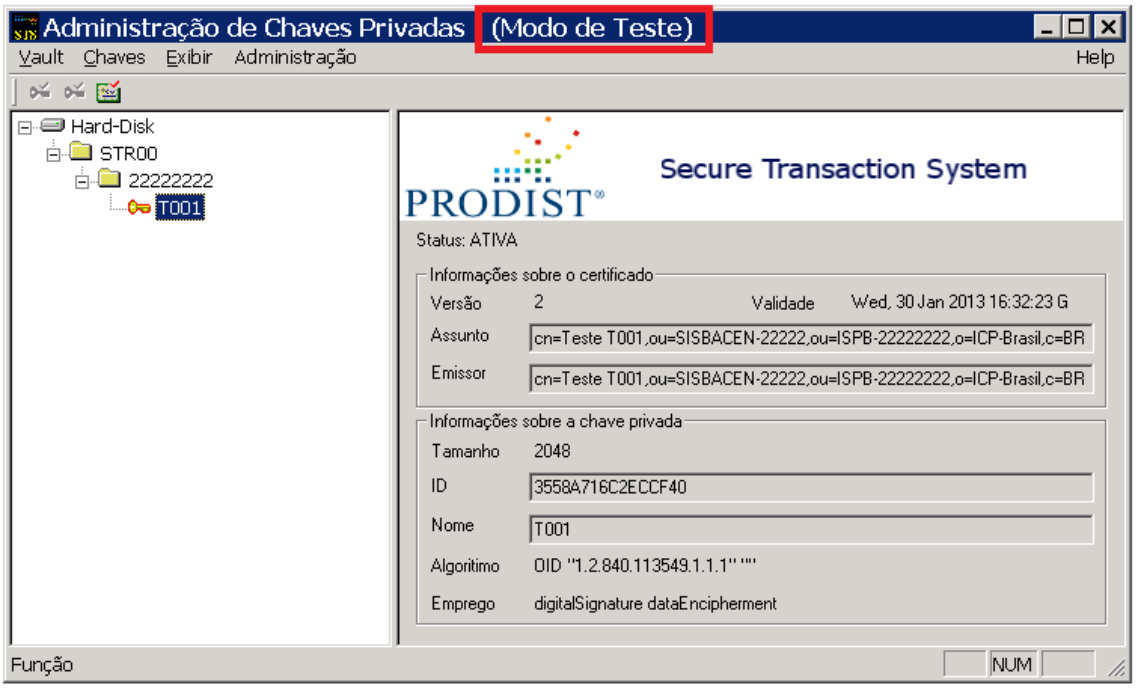
Em seguida clique duas vezes sobre a pasta que identifica o ISPB da instituição proprietária do certificado que será exportado e salve o arquivo de certificado **SEMPRE** com o nome **"00000000.cer"** (oito dígitos zero), clicando no botão **[Salvar]**.

Ex.: **STR00\11111111\00000000.cer**

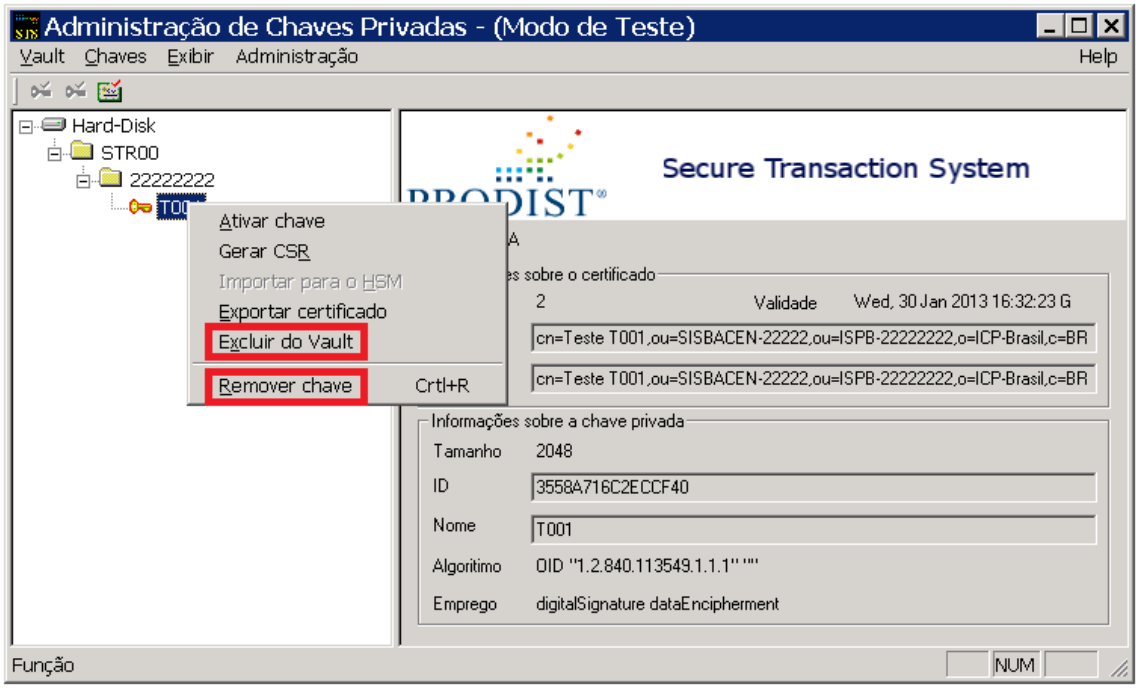


5.7.4 Excluindo chaves

Para realizar a exclusão de uma chave dentro do aplicativo **<Administração de Chaves Privadas>**, primeiro é preciso ativar o "**Modo de Teste"** da interface**.** <Mantenha as teclas **[Ctrl]** + **[Shift]** pressionadas e então aperte cinco vezes a tecla **[Insert]**. A Barra de identificação da janela será alterada e a inscrição Modo de Teste aparecerá no título da janela:



Clique com o botão direito do mouse em cima do ícone da chave que deseja excluir e aparecerão duas opções de exclusão - **[Excluir do Vault]** e **[Remover chave].**

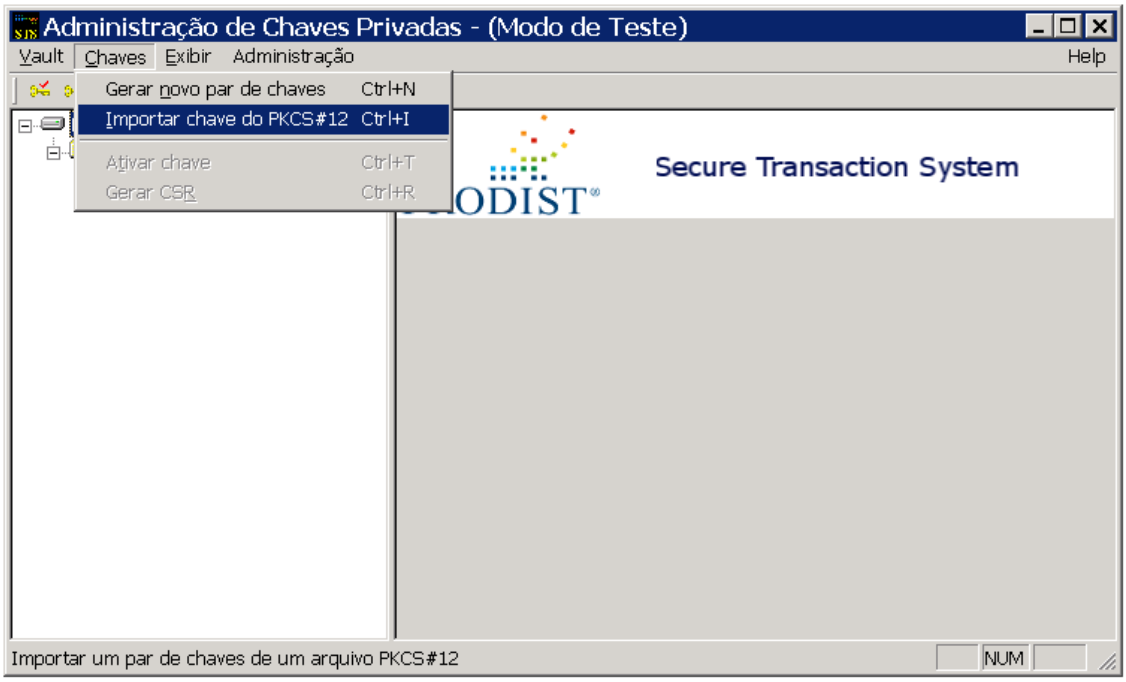


- **[Excluir do Vault]**: Esta opção fará com que os dados da chave sejam excluídos de dentro do arquivo **"vault.sts"**, permanecendo, assim, o arquivo correspondente, de sufixo **".p12",** dentro da pasta **"\Prodist\STS RSFN\Servidor\Vault"** do servidor.
- **[Remover chave]**: Essa opção fará a completa exclusão da chave, removendo seus dados do arquivo **"vault.sts"** e também o arquivo correspondente, de sufixo **".p12",** que estiver dentro da pasta **"\Prodist\STS RSFN\Servidor\Vault"** do servidor.

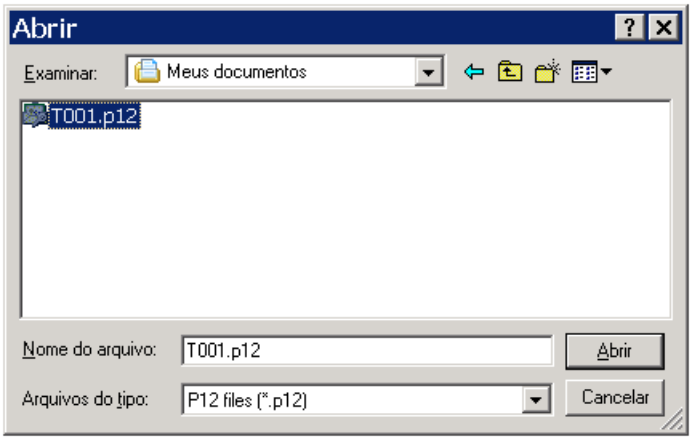
5.7.5 Importação de chaves

5.7.5.1 Importando e ativando um par de chaves armazenado em arquivo PKCS#12 (.p12) para o repositório de disco rígido (Vault)

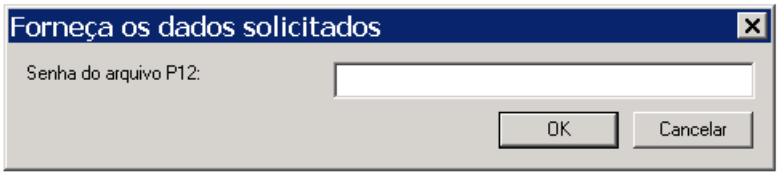
Para importar um par de chaves que ficará armazenado no disco rígido, será necessário utilizar o aplicativo **<Administração de Chaves Privadas>**. Clique na opção "**Chaves**" do menu superior e em seguida, escolha a opção "**Importar chave do PKCS#12**" no menu suspenso.



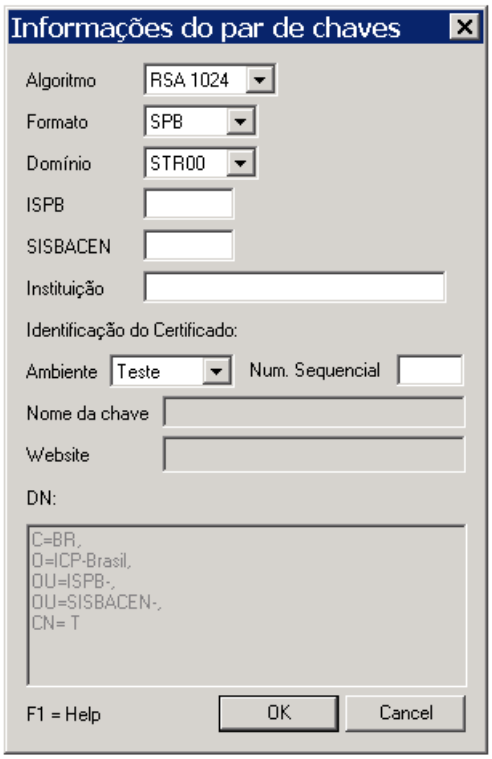
Navegue pela janela do **<Explorer>** até a localização do arquivo com o sufixo **“.p12”** que você deseja importar e clique no botão **[Abrir]**.



A senha deste arquivo lhe será solicitada através de uma janela similar a janela listada a seguir. Preencha o campo “**Senha do Arquivo P12**” com a senha atribuída a esta chave no momento de sua criação e em seguida clique no botão **[OK]**.



O aplicativo irá exibir a janela **informações da chave** onde você deverá informar os detalhes da chave que estiver sendo importada. Preencha os campos solicitados e clique no botão **[OK]**.



A chave importada poderá ser visualizada do lado esquerdo da janela principal do aplicativo **<Administração de Chaves Privadas>**.

IMPORTANTE: Certifique-se de que não haja nenhum arquivo com o mesmo nome do par de chaves a ser importado (Ex.: **`T001, P001, T002, P002`**...) localizado dentro da pasta **`"vault"`**, que por padrão fica localizada em: **`"c:\program files\prodist\sts rsfn\servidor\vault[...]"`** (Note que o caminho da pasta **`"vault"`** pode ser diferente dependendo da versão do Windows).
Caso você tente realizar a importação de um par de chaves já existente na pasta **`"vault"`**, será exibida a seguinte mensagem de erro:

ATENÇÃO! Antes que a chave possa ser utilizada pelo **Servidor STS**, é necessário ativá-la e, logo após**, reiniciar o Servidor STS**.

5.7.6 Importando chaves para os HSM Safenet LUNA SA e nCipher netHSM

Para importar chaves para estes HSM utilize os seguintes aplicativos que foram distribuídos junto com o **STS RSFN**:

Safenet Luna SA	`LunaImportP12.exe`
nCipher netHSM	`nethsmkeyimport.exe`

Estes aplicativos encontram-se na subpasta "**Servidor**" da pasta de instalação do **STS RSFN**.

O manual de integração do **STS RSFN** com o HSM correspondente possui maiores detalhes sobre esta operação.

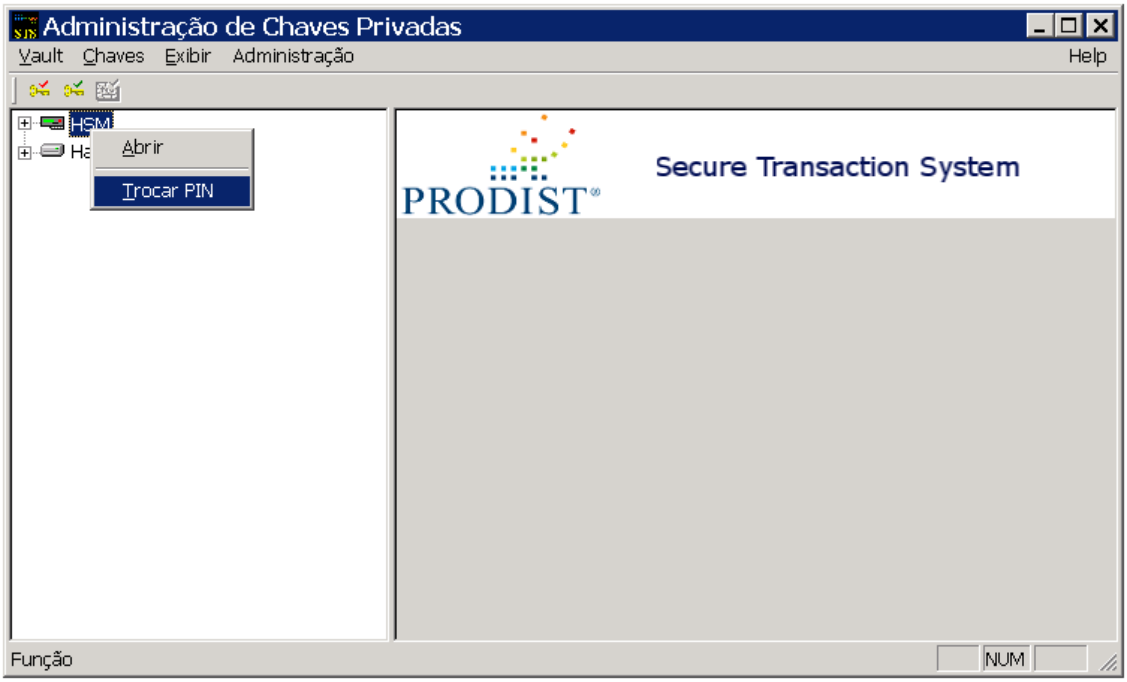
5.7.7 Trocando o PIN do HSM através do STS RSFN

Para trocar o PIN (senha) de um HSM, é necessário certificar-se de que não exista nenhuma sessão em andamento com o HSM.

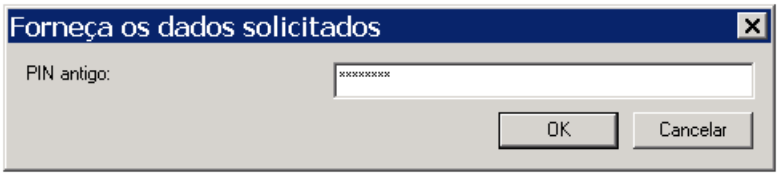
5.7.7.1 Trocando o PIN do HSM Baltimore ou HSM nCipher

Execute o aplicativo **<Administração de Chaves Privadas>**.

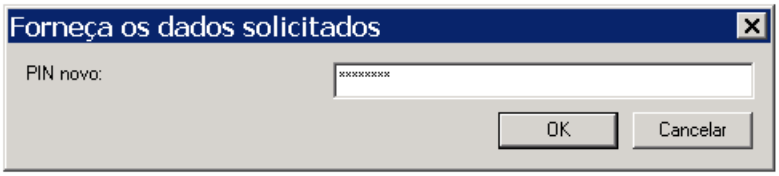
Clique com o botão direito do mouse sobre o ícone do HSM e em seguida clique sobre a opção "**Trocar PIN**".



Digite o PIN antigo e clique no botão **[OK]**.



A janela abaixo será exibida e você deverá digitar o novo PIN, clicando no botão **[OK]** para confirmar.



Confirme o novo PIN e clique no botão **[OK]**.

OBS – HSM nCipher: Caso vários Servidores STS estejam compartilhando as mesmas chaves privadas em um mesmo HSM nCipher, tenha em mente que **a troca do PIN feita em um servidor não é refletida nos outros servidores.** Neste caso, após trocar o PIN no primeiro

servidor, copie o arquivo **{vault.sts}** deste servidor para os outros servidores que compartilham o mesmo HSM.

5.7.7.2 Trocando o PIN do HSM Luna SA

A troca de PIN do HSM LUNA SA **não pode ser feita através do STS RSFN. Ela deve ser feita diretamente através do HSM**, seguindo as instruções fornecidas no manual do HSM LunaSA.

Após efetuar a troca do PIN diretamente no HSM, execute os passos a seguir:

1. Abra o aplicativo **<Administração de Chaves Privadas>.**
2. Dê um duplo clique no ícone HSM.
3. Insira a novo PIN do HSM.
4. Aguarde a abertura dos Domínios e suas respectivas chaves dentro do HSM.
5. Encerre a execução do aplicativo **<Administração de Chaves Privadas>.**

5.7.8 Gerando uma Requisição de Certificado (CSR) para par de chaves RSA 1024

Após a geração do par de chaves é necessário gerar o CSR (Certificate Signing Request) do certificado digital a ser emitido por uma Autoridade Certificadora. No âmbito da RSFN (Rede do Sistema Financeiro Nacional) é obrigatório o uso de certificado emitido por certificadora que pertença a ICP-Brasil. Existem diversas Autoridades Certificadoras que fazem parte desta infraestrutura e a instituição financeira pode escolher qualquer uma das certificadoras credenciadas.

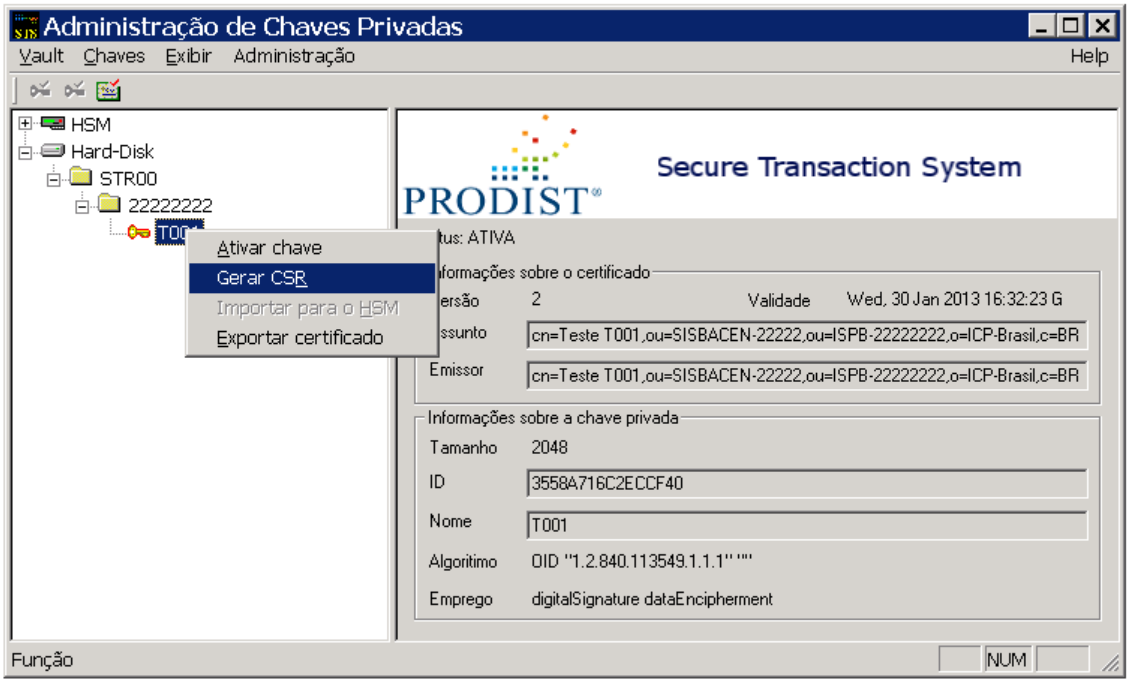
A CSR é um conjunto de dados que contém informações sobre o proprietário do certificado e sua chave pública.

Cada Autoridade Certificadora tem seu próprio processo de recepção de CSR e emissão de certificados, mas em geral, elas possuem um formulário web, através do qual as instituições podem postar o conteúdo de suas CSR.

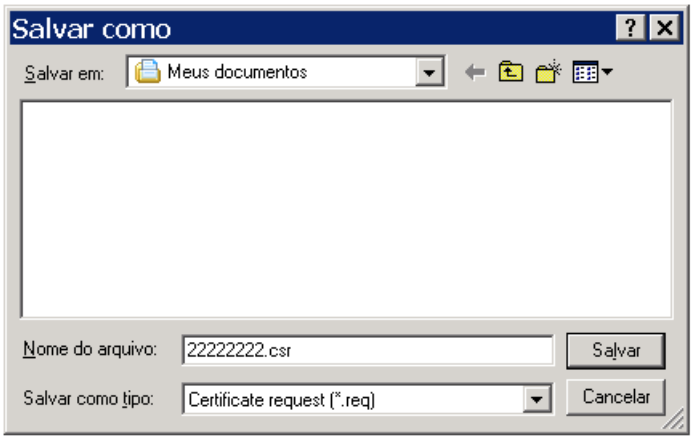
Para gerar um arquivo de Requisição de Certificado Assinado (CSR), para par de chaves RSA 2048, utilize os procedimentos descritos no item 5.7.9.

Para gerar um arquivo de Requisição de Certificado Assinado (CSR), para par de chaves padrão RSA 1024, você deve utilizar o aplicativo **<Administração de Chaves Privadas>**.

Após identificar a chave privada para a qual você deseja solicitar a emissão de certificado digital, junto a Autoridade Certificadora, posicione o ponteiro do mouse sobre ela e clique com o botão direito. Ao ser exibido o menu suspenso, selecione a opção ”***Gerar CSR***“ conforme indicado na figura a seguir:



Indique o nome do arquivo (sugerimos que seja o ISPB da instituição) e o diretório onde ele deverá ser salvo. Em seguida clique no botão **[Salvar]**. Veja exemplo a seguir:



Após a geração da CSR, que neste caso é um arquivo de sufixo **“.req”**, siga as recomendações da Autoridade Certificadora de sua escolha, de forma a garantir o correto envio das informações necessárias à geração do certificado digital de sua instituição.

5.7.9 Gerando uma Requisição de Certificado (CSR) para par de chaves RSA 2048

Para gerar um arquivo de Requisição de Certificado Assinado (CSR), para um par de chaves RSA 2048, você deve utilizar o aplicativo **<csr_tui.exe>**. Este aplicativo está localizado na mesma pasta do servidor do **STS RSFN(…Prodist\STS RSFN\Servidor)**.

Para gerar o arquivo de sufixo **"`.csr`"** você precisará abrir uma janela de *prompt* de comando, ir até a pasta de instalação do **<csr_tui>** e executar um comando similar ao exemplo abaixo:

```
csr_tui.exe -d STR00 -k 12345678 -n T001 -s "CN=PRODIST T001,OU=SISBACEN-
12345,OU=ISPB-12345678,O=ICP-Brasil,C=BR" -o PRODIST.txt
```

Onde:

`-d` = Domínio para o qual o certificado será utilizado.

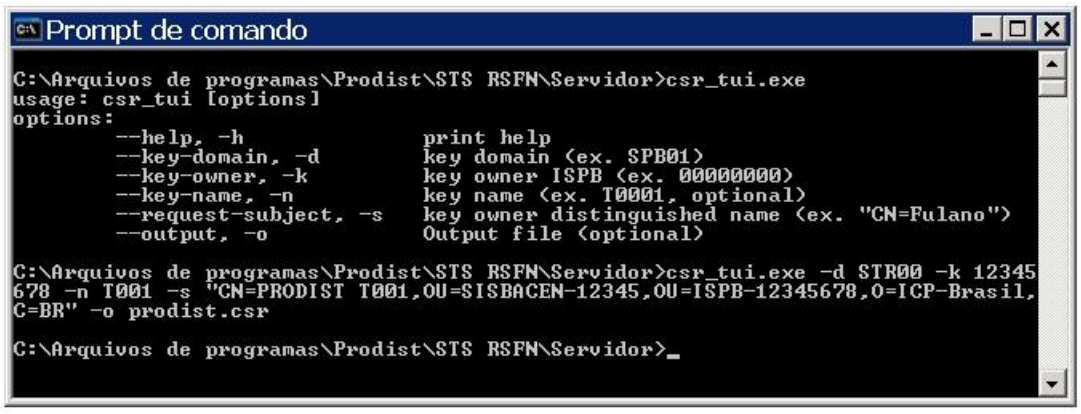
`-k` = ISPB da chave.

`-n (opcional)`: Nome da chave. Quando iniciado com o parâmetro **"`T`"**, refere-se a chaves de homologação e quando iniciado com o **"`P`"**, refere-se a chaves de produção.

`-s:` *Distinguished Name* - são dados da Instituição que ficam gravadas no certificado que no SPB é composta de 4 campos obrigatórios: CN, OU, O e C.

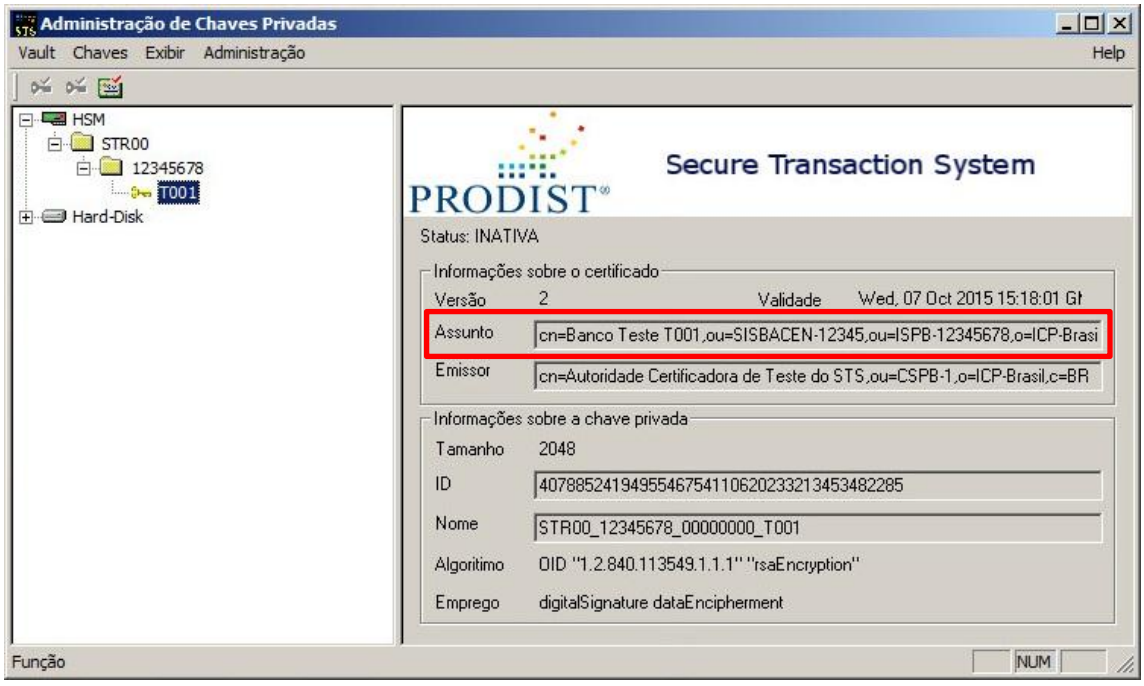
`-o (opcional):` Nome do arquivo de saída que será gerado pela aplicação **<csr_tui>**, caso não seja preenchido, o mesmo será impresso na janela do prompt.

Exemplo ilustrativo:



OBS: Ao preencher o parâmetro ***"-s" (Distinguished Name)***, certifique-se de **não colocar ESPAÇO** entre as vírgulas.

As informações sobre a chave devem ser preenchidas de acordo com a aplicação **<Administração de Chaves Privadas>**.



NOTA: O arquivo **“.csr”** poderá ser criado tanto a partir de uma chave criada em hardware (HSM) quanto em software (Hard-disk).

1) Após a execução do comando você poderá encontrar o arquivo de saída na pasta onde o **<csr_tui>** foi executado, por padrão **“…Prodist\STS RSFN\Servidor”**.

2) O arquivo de sufixo **“.csr”,** ou seu conteúdo, deverá ser utilizado junto à Autoridade Certificadora de sua escolha para a obtenção do Certificado Digital.

OBS: A CSR gerada pela aplicação **<csr_tui>** sempre será assinada com o algoritmo de *hash* SHA-256.

5.8 LOAD BALANCE (BALANCEAMENTO DE CARGA)

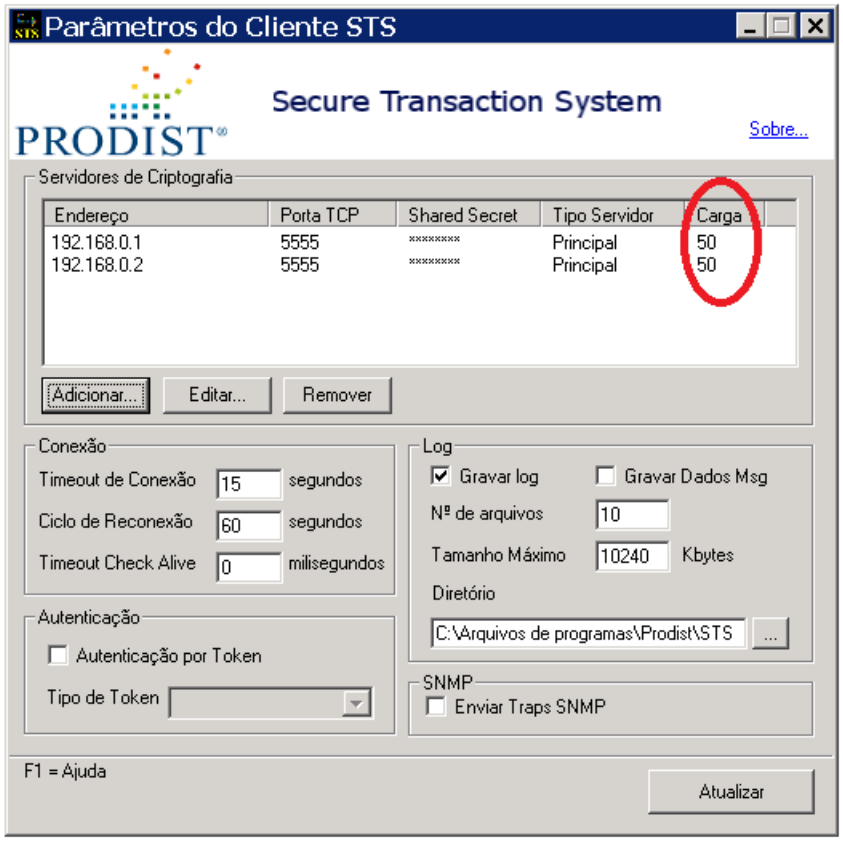
O balanceamento de carga é uma funcionalidade disponível no STS RSFN para aquelas instituições que possuam mais de uma licença de produção do produto e que pretendam

distribuir a carga de processamento entre dois ou mais servidores, de forma a garantir um melhor desempenho e/ou alta disponibilidade.

A configuração de *Load Balance* pressupõe que os servidores envolvidos irão trabalhar em Alta Disponibilidade (*Failover*), ou seja, ao habilitar o *Load Balance* você estará habilitando também o *Failover*.

A distribuição da carga é feita pela atribuição do percentual de carga que cada servidor do conjunto deverá processar. Esta configuração é feita nas máquinas "cliente", ou seja, aquelas que executam uma aplicação **Cliente STS**.

Os parâmetros de configuração de cada "cliente" devem incluir os endereços IP dos servidores que aquele cliente irá utilizar e, através do aplicativo **<Parâmetros do Cliente>**, a cada servidor deve estar associada (em percentuais) a carga de processamento que deverá ser a ele enviada. Por exemplo, se forem utilizados dois servidores, a carga pode ser distribuída em 50% para cada servidor. Veja figura a seguir:

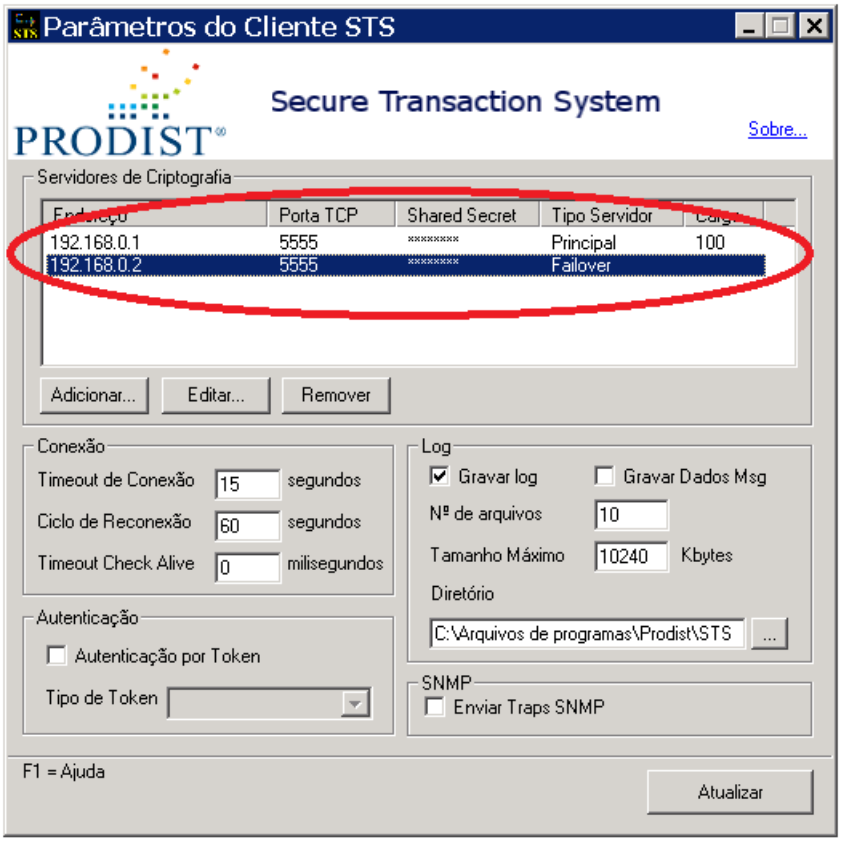


IMPORTANTE: O endereço IP da máquina "cliente" deve estar autorizado em cada servidor do conjunto. Utilize o aplicativo **<Parâmetros do Servidor STS>**, em cada servidor, e insira os endereços IP das máquinas clientes na lista de "**Clientes Autorizados**".

5.9 FAILOVER

O *Failover* é uma funcionalidade disponível no STS para aquelas instituições que possuam apenas uma licença de produção do produto, mas que desejam contar com um servidor de backup (secundário), em modo *standby*, para os casos de falha do servidor principal.

Quando esta configuração é feita, caso o servidor principal não responda em tempo hábil ou retorne erros na criptografia (ex: problemas com o HSM), o servidor secundário (*Failover*) é ativado e passa a tratar todas as requisições que seriam normalmente enviadas ao servidor principal. Em intervalos regulares de tempo, o servidor principal é testado e, caso já esteja apto a realizar suas funções, o(s) servidor(es) secundário(s) (*Failover*) voltará(ão) ao estado *standby*.



5.10 CONSOLE DE TESTE

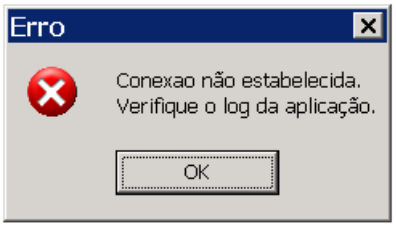
Um aplicativo de suma importância que é distribuído com a instalação original do STS é o **<Console de Teste>**. Sua principal função é verificar se o produto está instalado e configurado de maneira adequada.

Após fazer todas as configurações dos módulos servidor e cliente e também de ter criado chaves e certificados, é conveniente que você teste a consistência do sistema através deste aplicativo.

Para executar a **<Console de Teste>** clique em **`Iniciar > Todos os Programas > Prodist > STS RSFN > Cliente > Console de Teste.`**

O primeiro teste que será realizado está relacionado com a conectividade entre o Servidor STS e o Cliente STS.

Se ao executar o aplicativo aparecer a mensagem "**Conexão não estabelecida**" (ilustrada abaixo), isso indicará que as configurações do Servidor e/ou Cliente STS ainda não estão corretas.

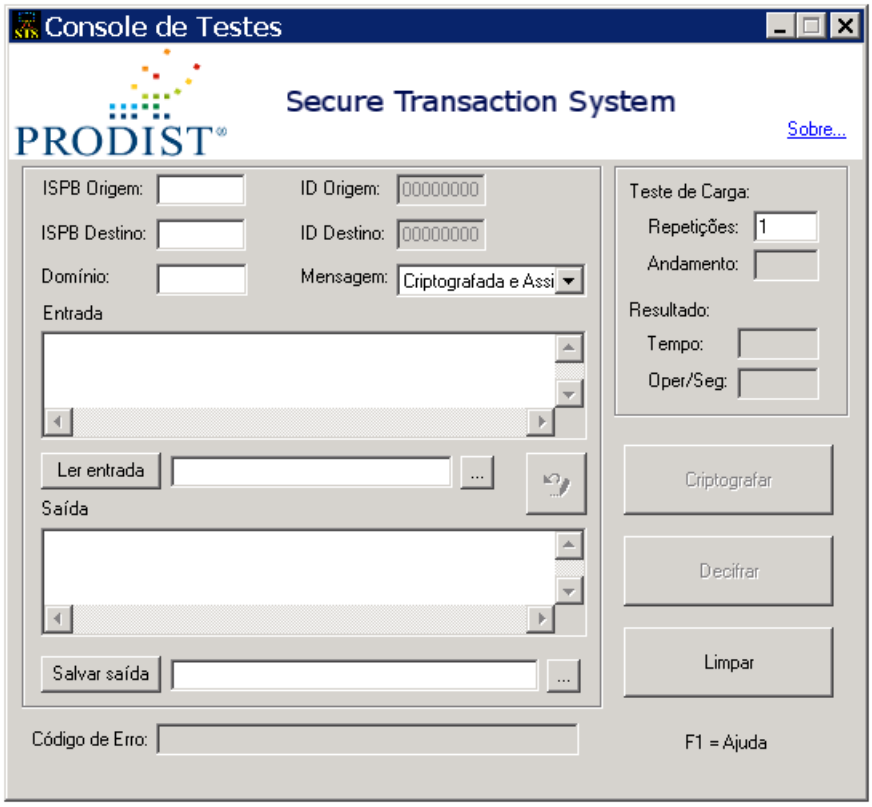


Esta mensagem indica uma falha na configuração da conexão TCP/IP entre o Cliente e o **Servidor STS**. Para reparar esta configuração, verifique os seguintes passos:

- Na máquina do cliente, execute o aplicativo de configuração **<Parâmetros do Cliente STS>** e verifique se o endereço IP e porta TCP para conexão estão corretamente configurados.
- Verifique se o meio físico (rede) entre a máquina do cliente e a máquina do Servidor STS está OK. Para isto, a partir da máquina do cliente, execute um comando **PING** contra o IP da máquina do servidor.
- Verifique se o endereço IP da máquina do cliente está autorizado para conexão com o servidor. Para fazer isto execute o aplicativo de configuração **<Parâmetros do Servidor STS>** e verifique se o endereço IP da máquina do cliente consta da relação de Clientes Autorizados. Caso não conste, preencha uma das caixas de clientes autorizados com o endereço IP do cliente em questão, confirme e então clique no botão **[Atualizar]** para salvar as alterações realizadas.
- Verifique se as "***Shared Secret***" das máquinas **Cliente e Servidor STS** estão iguais. Como não há como ver o conteúdo de uma ***Shared Secret***, preencha novamente estas caixas nos aplicativos de configuração de **Parâmetros do Cliente e do Servidor STS**. Clique no botão **[Atualizar]** em ambos os aplicativos após ter realizado as alterações.

- Reinicialize o sistema (*reboot*) no computador onde o **Servidor STS** foi instalado.
- Verifique se os seguintes serviços estão iniciados:
  - Na máquina do **Servidor STS**, verifique o serviço "**STSServer RSFN**";
  - Na máquina onde foi instalado o **Cliente STS**, verifique o serviço "**STSClient RSFN**";

Verificados os passos acima, tente novamente executar a console de testes e a janela a seguir deverá surgir:



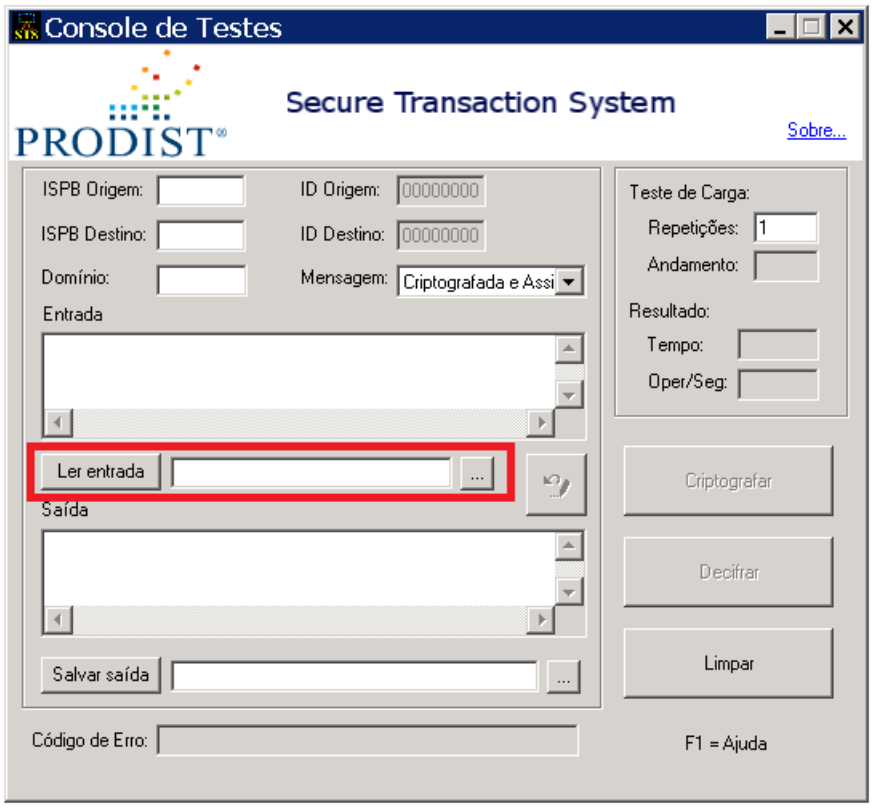
5.10.1 Teste de criptografia

Antes de realizar qualquer teste de criptografia, tenha certeza de ter criado chaves e certificados válidos. Não se esqueça de ativar a chave privada através do aplicativo **<Administração de Chaves Privadas>**.

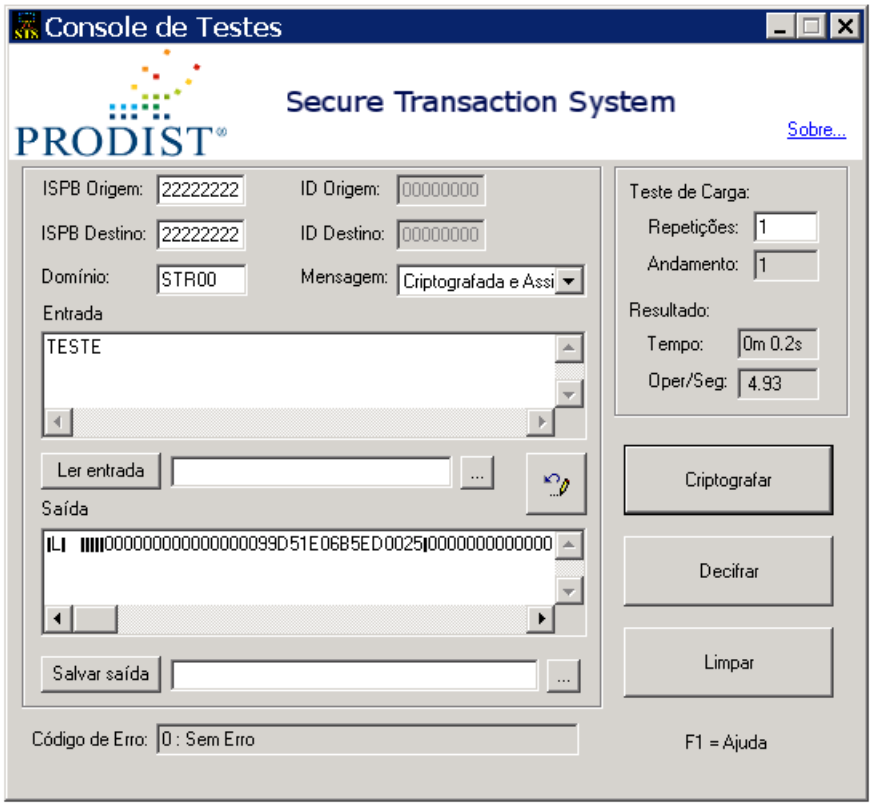
- Preencha os campos "**ISPB Origem**" e "**ISPB Destino**" com códigos de instituições para as quais você tenha certificados instalados em seu ambiente. Para efeito de teste, você pode utilizar o ISPB de sua própria instituição, tanto como "**ISPB Origem**" como

"**ISPB Destino**". O teste feito desta maneira irá possibilitar que você criptografe e também decriptografe os pacotes gerados.

- Preencha o campo "**Domínio**" com os 05 (cinco) caracteres alfanuméricos que identificam o domínio envolvido na operação que será realizada.
- Preencha o campo "**Tipo de Mensagem na Criptografia**" com a opção **"Criptografada e assinada**";
- Preencha o campo "**Entrada**" com um conjunto de caracteres (Ex.: "TESTE") a ser criptografado. Se preferir, você pode orientar o aplicativo para que leia os dados de um determinado arquivo (seja ele texto ou binário), selecionando-o no botão  . Utilize o botão **[Ler Entrada]** para que o **<Console de Testes>** identifique os dados e os adicione no campo **"Entrada"**.



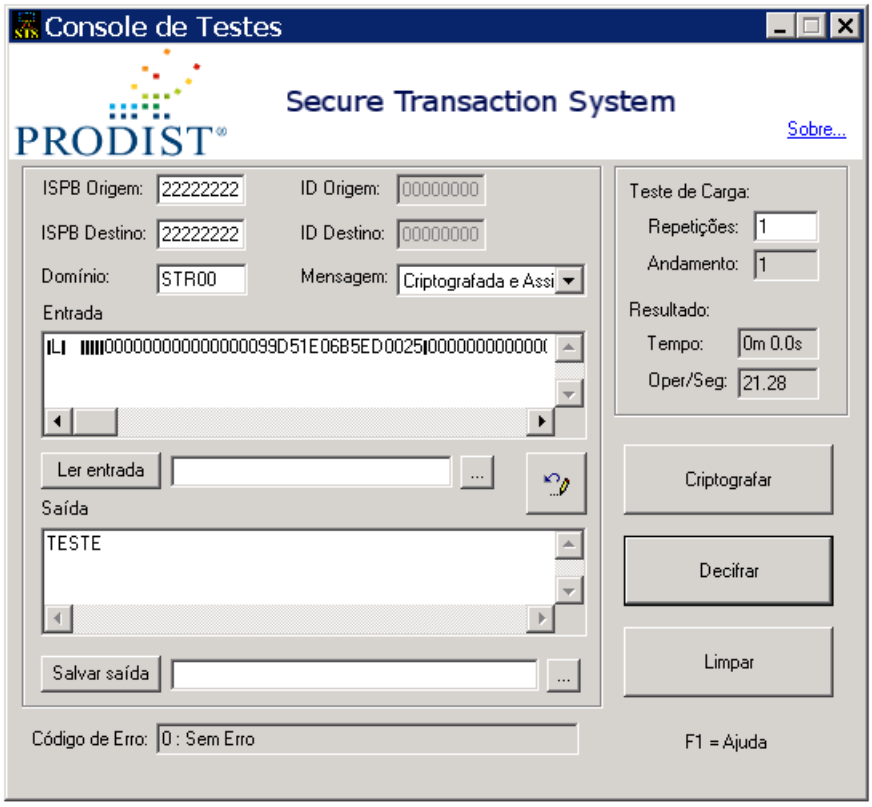
- Clique no botão **[Criptografar]**. O Resultado da criptografia aparecerá na caixa "**Saída**".
- Se quiser copiar o conteúdo da caixa "**Saída**" para a caixa "**Entrada**", clique no botão  localizado ao lado esquerdo do botão **[Criptografar]**.



5.10.2 Teste de decriptografia

- Preencha o campo "**Entrada**" com um conjunto de caracteres que represente algum dado que já tenha sido criptografado. Se preferir, você pode abrir o conteúdo de um determinado arquivo (seja ele texto ou binário), clicando no botão  e selecionando-o. Utilize o botão **[Ler Entrada]** para que o **<Console de Testes>** identifique os dados criptografados e os adicione no campo **"Entrada".**
- Preencha o campo "**Domínio**" com os 05 (cinco) caracteres alfanuméricos que identificam o domínio envolvido na operação que será realizada.
- Preencha o campo "**Tipo de Mensagem na Criptografia**" com a opção **"Criptografada e assinada**";
- Caso você tenha acabado de criptografar um conjunto de caracteres e queira copiar o conteúdo da caixa "**Saída**" para a caixa "**Entrada**", clique no botão  localizado ao lado do botão **[Criptografar]**.

- Clique no botão **[Decifrar]** e então o resultado da decriptografia aparecerá na caixa "**Saída**".



5.10.3 Simulação de GEN0001 - IF requisita Teste de conectividade – ECO

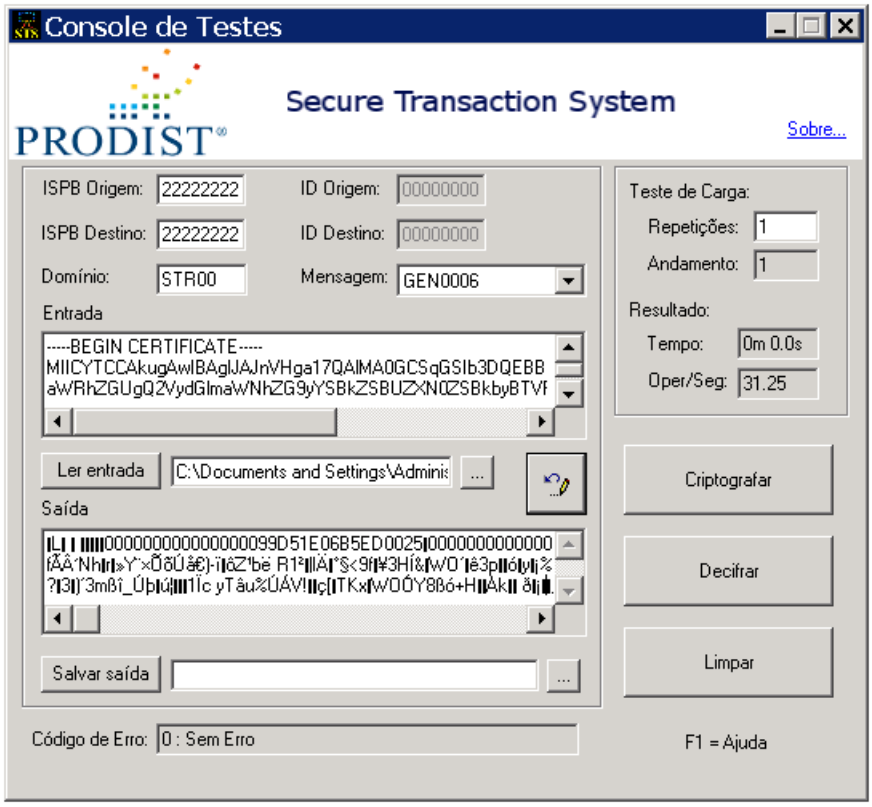
- Preencha os campos "**ISPB Origem**" e "**ISPB Destino**".
- Preencha o campo "**Domínio**" com os 05 (cinco) caracteres alfanuméricos que identificam o domínio envolvido na operação que será realizada.
- Preencha o campo "**Tipo de Mensagem na Criptografia**" com a opção "**Em Claro (Assinada)**".
- Preencha o campo "**Entrada**" com uma mensagem GEN0001. Se preferir, leia a mensagem a partir de um arquivo, selecionando com o botão ... e depois clicando no botão **[Ler Entrada]**.
- Clique no botão **[Criptografar]**. O Resultado da criptografia aparecerá na caixa "**Saída**".

5.10.4 Simulação de GEN0004 - GEN informa Erro de transmissão na mensagem

- Preencha os campos "**ISPB Origem**" e "**ISPB Destino**".
- Preencha o campo "**Domínio**" com os 05 (cinco) caracteres alfanuméricos que identificam o domínio envolvido na operação que será realizada.
- Preencha o campo "**Tipo de Mensagem na Criptografia**" com a opção **"GEN0004"**;
- Preencha o campo "**Entrada**" com a **GEN0004**. Se preferir, selecione-a com o botão  e então clique no botão **[Ler Entrada]**.
- Clique no botão **[Criptografar]**. O Resultado da criptografia aparecerá na caixa "**Saída**".

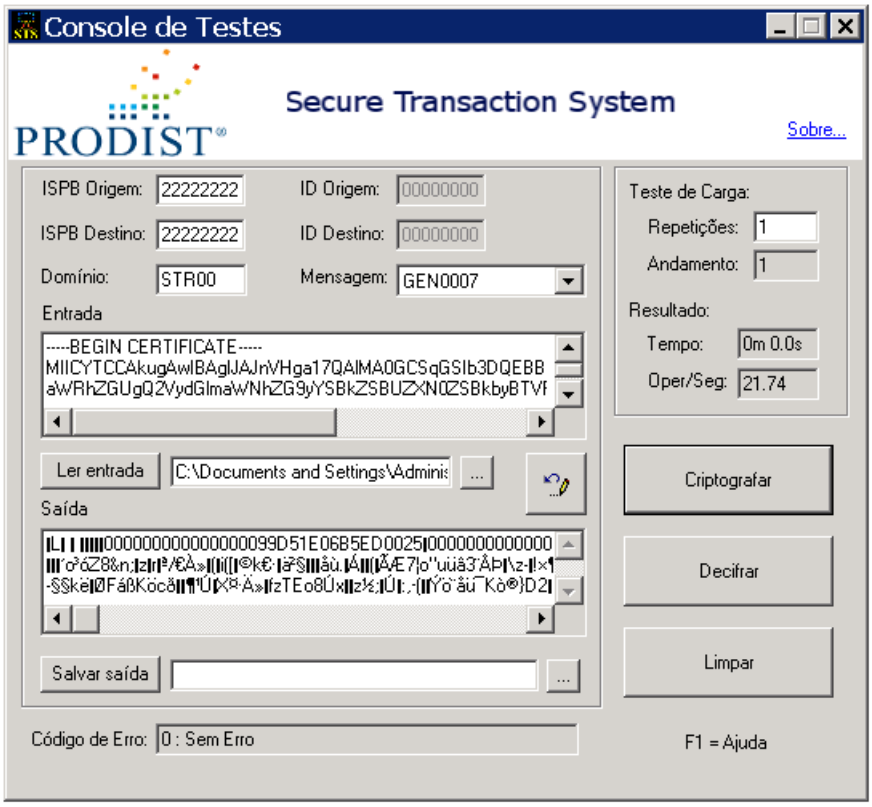
5.10.5 Simulação de GEN0006 – IF informa Atualização da situação dos certificados digitais

- Preencha os campos "**ISPB Origem**" e "**ISPB Destino**".
- Preencha o campo "**Domínio**" com os 05 (cinco) caracteres que identificam o domínio envolvido na operação que será realizada.
- Preencha o campo "**Tipo de Mensagem na Criptografia**" com a opção **"GEN0006"**;
- Preencha o campo **"Entrada"** com o conteúdo do certificado, desde **-----BEGIN CERTIFICATE-----** até o **-----END CERTIFICATE-----.** Se preferir, selecione algum arquivo que tenha o mesmo conteúdo com o botão  e então clique no botão **[Ler Entrada]** para que os dados sejam lidos e adicionados no campo **"Entrada"**.
- Clique no botão **[Criptografar]**. O Resultado da criptografia aparecerá na caixa "**Saída**".

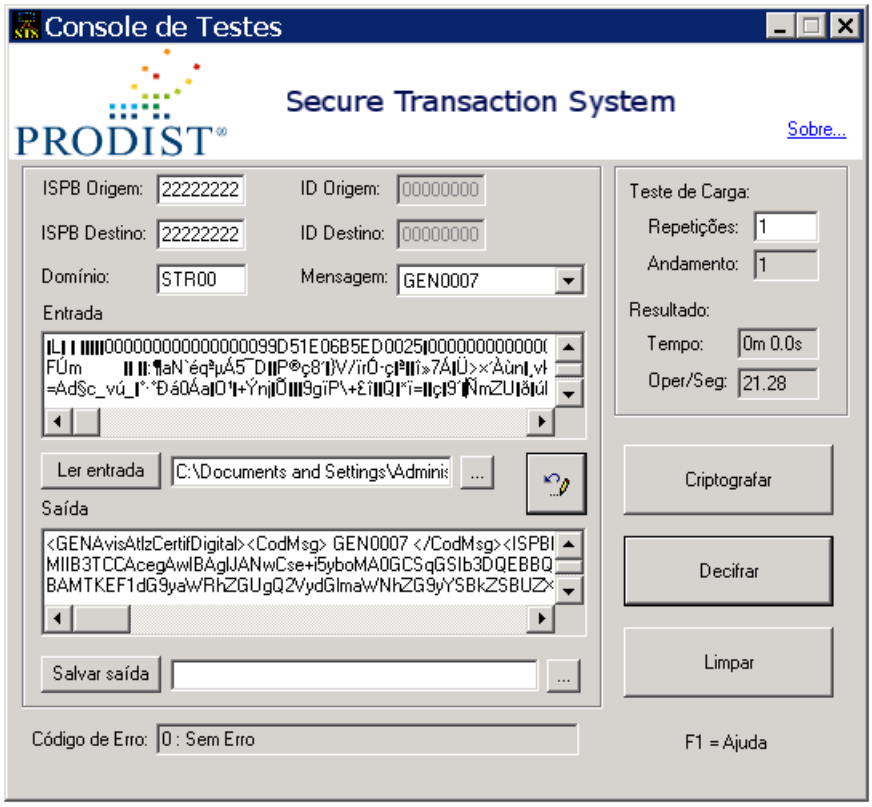


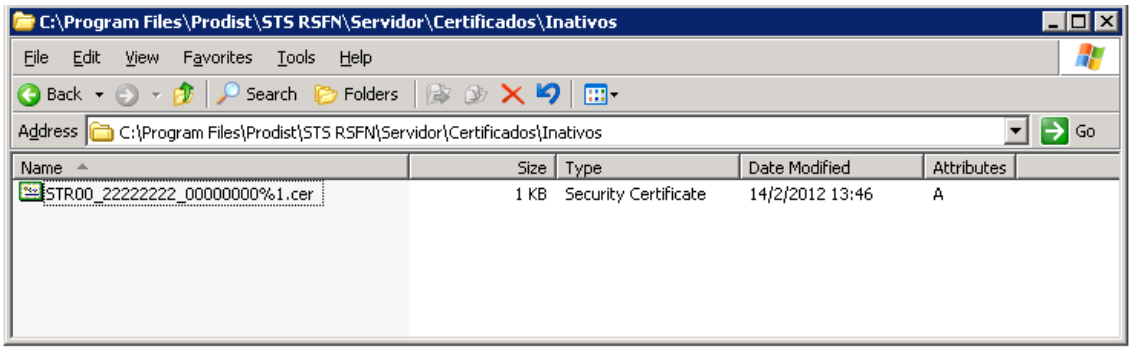
5.10.6 Simulação de GEN0007 - GEN avisa Atualização de certificado digital

- Preencha os campos "**ISPB Origem**" e "**ISPB Destino**".
- Preencha o campo "**Domínio**" com os 05 (cinco) caracteres alfanuméricos que identificam o domínio envolvido na operação que será realizada.
- Preencha o campo "**Tipo de Mensagem na Criptografia**" com a opção **"GEN0007";**
- Preencha o campo "**Entrada**" com o conteúdo do certificado, desde **-----BEGIN CERTIFICATE-----** até o **-----END CERTIFICATE-----.** Se preferir, selecione algum arquivo que tenha o mesmo conteúdo com o botão ... e então clique no botão **[Ler Entrada]** para que os dados sejam lidos e adicionados no campo **"Entrada"**.
- Clique no botão **[Criptografar]**. O Resultado da Criptografia aparecerá na caixa "**Saída**".



- Copie o conteúdo da caixa "**Saída**" para a caixa "**Entrada**", clicando no botão  localizado ao lado do botão **[Criptografar]**.
- Clique no botão **[Decifrar]**. O Resultado da decriptografia aparecerá na caixa "**Saída**". O novo certificado será salvo pelo STS no diretório configurado pelo aplicativo **<Parâmetros do Servidor>** e o certificado antigo será movido para a pasta "**Inativos**" localizada dentro da pasta **"Certificados"**.





5.11 ANÁLISE DE LOG

Embora a **PRODIST** tenha um rigoroso processo de testes de seus produtos, ocasionalmente, erros podem acontecer. Às vezes o erro pode estar relacionado com os nossos próprios aplicativos e outras com a configuração do ambiente do usuário. Para garantir um suporte ágil e efetivo, o Servidor STS foi dotado de um aplicativo de coleta de dados da máquina onde estiver instalado. Este aplicativo coleta todos os dados necessários para um pronto atendimento pelo suporte da **PRODIST**.

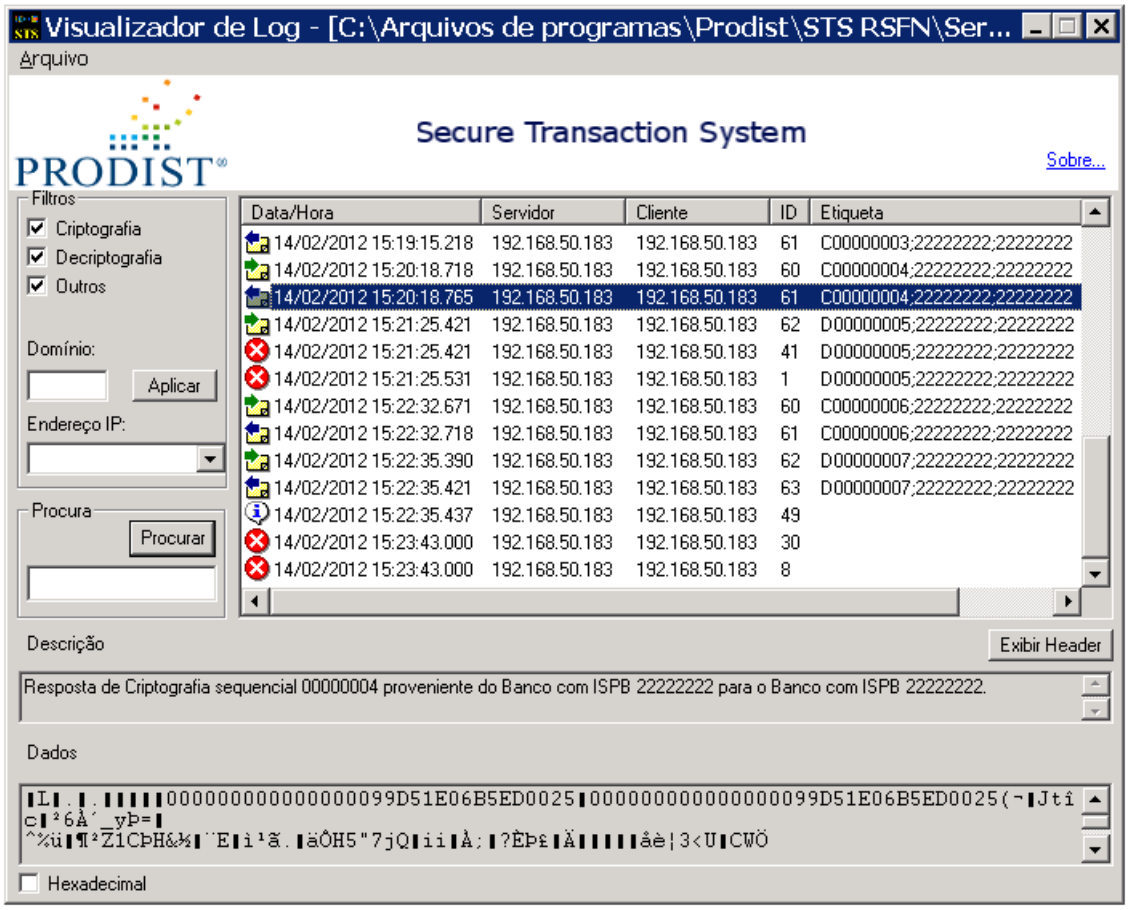
Também faz parte do STS um aplicativo para a visualização dos arquivos de LOG gerados pelo Servidor e pelo Cliente STS.

A forma de utilização deste aplicativo está descrita a seguir.

5.11.1 Visualizador de Log

Este aplicativo de ser utilizado para examinar os eventos armazenados nos arquivos de LOG, gerados pelo Servidor e Cliente STS. Os quatro tipos de eventos que existem são:

- Informação;
- Aviso;
- Log de Operação;
- Erro;
- A utilização do aplicativo é bastante simples e está detalhada a seguir:

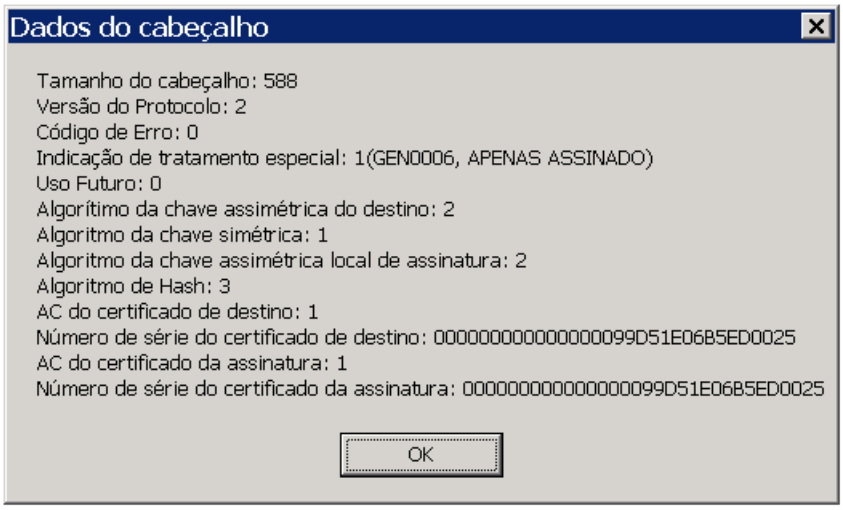


Clique no menu “**Arquivo**” e navegue até a localização do arquivo de LOG que deseja examinar. Este arquivo pode estar na subpasta “Log” da pasta “Servidor” ou da pasta “Cliente”.

Uma vez aberto o arquivo, os eventos nele existentes serão apresentados em duas seções da janela. A seção maior apresentará a lista de eventos encontrados no arquivo. A seção menor (logo abaixo) apresentará o conteúdo da mensagem de evento.

Clique em um dos eventos para ver seu conteúdo nas caixas “**Dados**” e “**Descrição**”.

- **Filtros:**
  - **Criptografia**: Se marcado, exibe somente os eventos de criptografia na lista.
  - **Decriptografia**: Se marcado, exibe somente os eventos de decriptografia na lista.
  - **Outros** : Se marcado, exibe somente os eventos de erro na lista.
  - **Dados da mensagem**: Se marcado, além do cabeçalho da mensagem exibe também o seu conteúdo.
  - **Domínio**: Preencha com o nome de um domínio para exibir apenas os eventos relacionados a ele.
  - **Endereço IP:** Utilize este filtro caixa para selecionar os eventos de um IP específico.
  - **Campo “Procura”:** Você deve utilizar este campo se desejar procurar um conjunto de caracteres específico no arquivo de LOG. Para isto basta digitar o conjunto de caracteres (ou palavras) que deseja encontrar e clicar no botão [**Procurar**]. Caso o conjunto de caracteres seja encontrado, o cursor será posicionado sobre o evento que o contém, na lista de eventos.
  - **Caixa “Hexadecimal”:** Marque esta caixa caso deseje examinar o conteúdo dos eventos em formato hexadecimal.
  - **Botão Exibir Header:** Exibe o header da mensagem em questão no formato a seguir:



6 Apêndices

6.1 Apêndice A – Noções de SNMP

O SNMP (Simple Network Management Protocol) é um protocolo da camada de aplicação designado para facilitar a troca de informações de gerenciamento entre dispositivos de rede. Usando os dados transportados pelo SNMP, os administradores de rede podem gerenciar mais facilmente a performance da rede, encontrar e solucionar problemas e planejar com mais precisão uma possível expansão da rede.

Atualmente, o SNMP é o protocolo mais popular para gerenciamento de diversas redes comerciais como as de universidades, centros de pesquisas e provedores de acesso e de informações. Esta popularização se deve ao fato de que o SNMP é um protocolo relativamente simples, porém suficientemente poderoso para resolver os difíceis problemas apresentados quando se tenta gerenciar redes heterogêneas.

6.2 Apêndice B – O arquivo vault.sts

O **“vault.sts”** é um arquivo criptografado onde são gravadas diversas informações sobre as chaves privadas utilizadas pelo Servidor STS, tais como o nome das chaves, senhas dos arquivos **“.p12”** (arquivos que guardam as chaves privadas armazenadas no Hard-Disk), password do HSM (quando utilizado), quais chaves estão ativas para cada ISPB, etc...

Este arquivo é criado quando o programa **“STSSeeder.exe”** é executado, após a instalação do Servidor STS. Ele é alterado sempre que alguma atualização é feita pelo aplicativo **<Administração de Chaves Privadas>**.

O arquivo **“vault.sts”** está relacionado com o arquivo **“Seed.p8”** que também é gerado pelo **“STSSeeder.exe”**.

Do ponto de vista de segurança, é de suma importância que os arquivos "STSSeeder.exe" e "Seed.p8" não permaneçam gravados no disco rígido de nenhum servidor.

Embora os arquivos **"STSSeeder.exe"** e **"Seed.p8"** não devam permanecer instalados no servidor, eles precisarão ser utilizados sempre que houver uma atualização (upgrade) do sistema STS RSFN.

6.3 Apêndice C – Entendendo os Arquivos de eventos

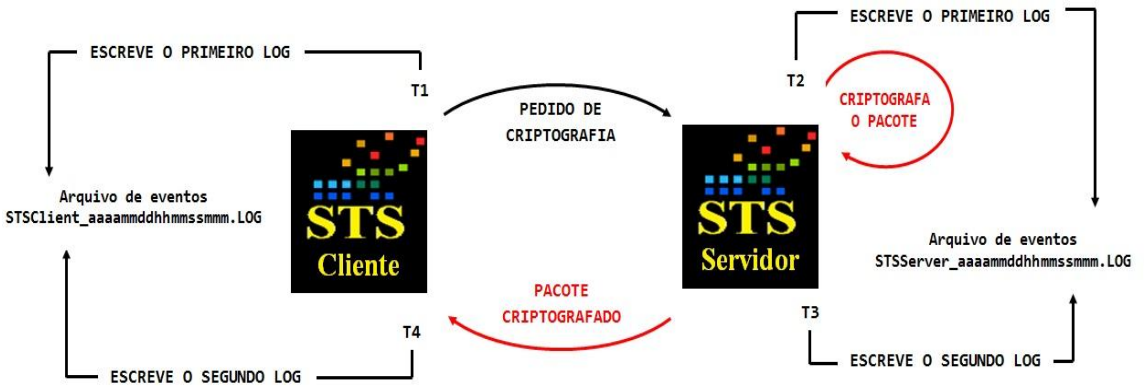
- **Nomenclatura dos arquivos de eventos**

`Nome do arquivo = [Tipo]_[Data/Hora no formato AAAAMMDDHHMMSSmmm].txt`
[Tipo]: **STSServer** para arquivos de eventos do Servidor STS ou **STSClient** para arquivos de eventos do Cliente STS.

- **Sequenciamento da gravação dos LOGs de eventos de criptografia e decriptografia**

Existe uma sequência lógica e um relacionamento no tempo para a gravação dos eventos de criptografia e decriptografia do **Servidor e do Cliente STS**. As figuras abaixo ilustram quais eventos são gravados (se estiverem ativos) e em quais momentos durante pedidos de criptografia e decriptografia.

a) Pedidos de Criptografia



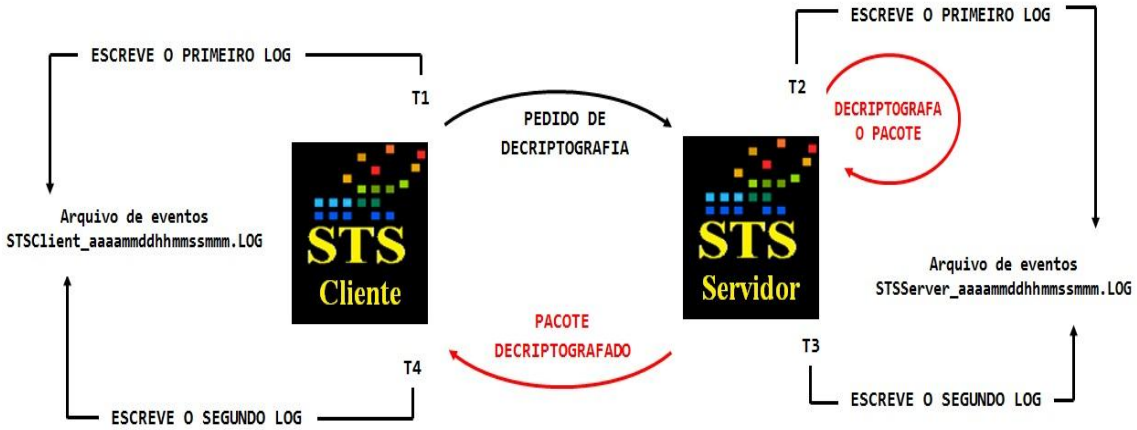
T1: Cliente STS envia pedido de criptografia ao Servidor STS. Neste momento é inserido um evento no arquivo de eventos do Cliente STS.

T2: Servidor STS recebe pedido de criptografia proveniente do Cliente STS. Neste momento é inserido um evento no arquivo de eventos do Servidor STS.

T3: Servidor STS executa a criptografia e envia pacote criptografado para o Cliente STS. Neste momento é inserido um evento no arquivo de LOG do Servidor STS.

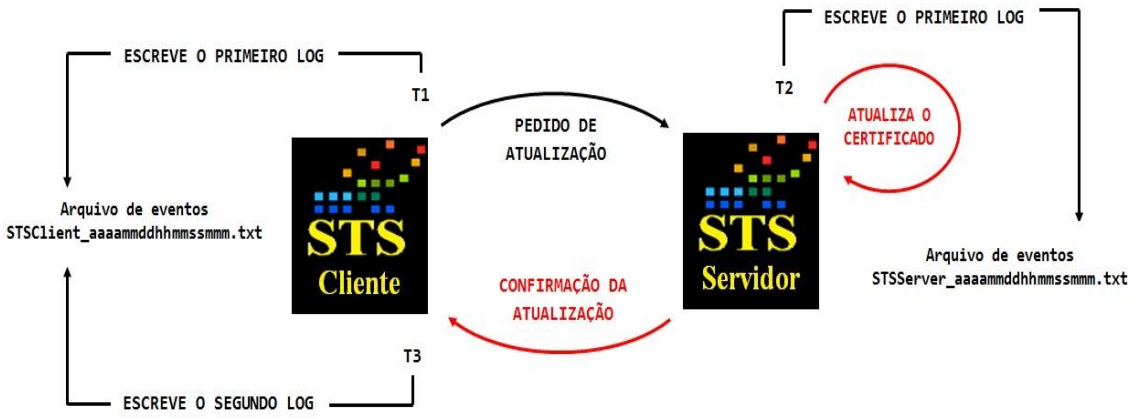
T4: Cliente STS recebe pacote criptografado proveniente do Servidor STS. Neste momento é inserido um evento no arquivo de eventos do Cliente STS.

b) Pedidos de Decriptografia



T1: Cliente STS envia pedido de decriptografia ao Servidor STS. Neste momento é inserido um evento no arquivo de eventos do Cliente STS.
T2: Servidor STS recebe pedido de decriptografia proveniente do Cliente STS. Neste momento é inserido um evento no arquivo de eventos do Servidor STS.
T3: Servidor STS executa a decriptografia e envia pacote decriptografado para o Cliente STS. Neste momento é inserido um evento no arquivo de eventos do Servidor STS.
T4: Cliente STS recebe pacote decriptografado proveniente do Servidor STS. Neste momento é inserido um evento no arquivo de eventos do Cliente STS.

c) Pedidos de Atualização de Certificado



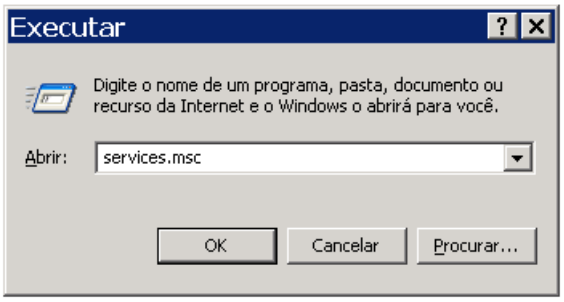
T1: Cliente STS envia pedido de atualização ao Servidor STS. Neste momento é inserido um evento no arquivo de eventos do Cliente STS.
T2: Servidor STS recebe pedido de atualização proveniente do Cliente STS e processa, atualizando o certificado da ISPB requisitada. Neste momento é inserido um evento no arquivo de eventos do Servidor STS.
T3: Cliente STS recebe confirmação de atualização de certificado proveniente do Servidor STS. Neste momento é inserido um evento no arquivo de eventos do Cliente STS.

6.4 Apêndice D – Alterando a configurações de execução do serviço STS RSFN.

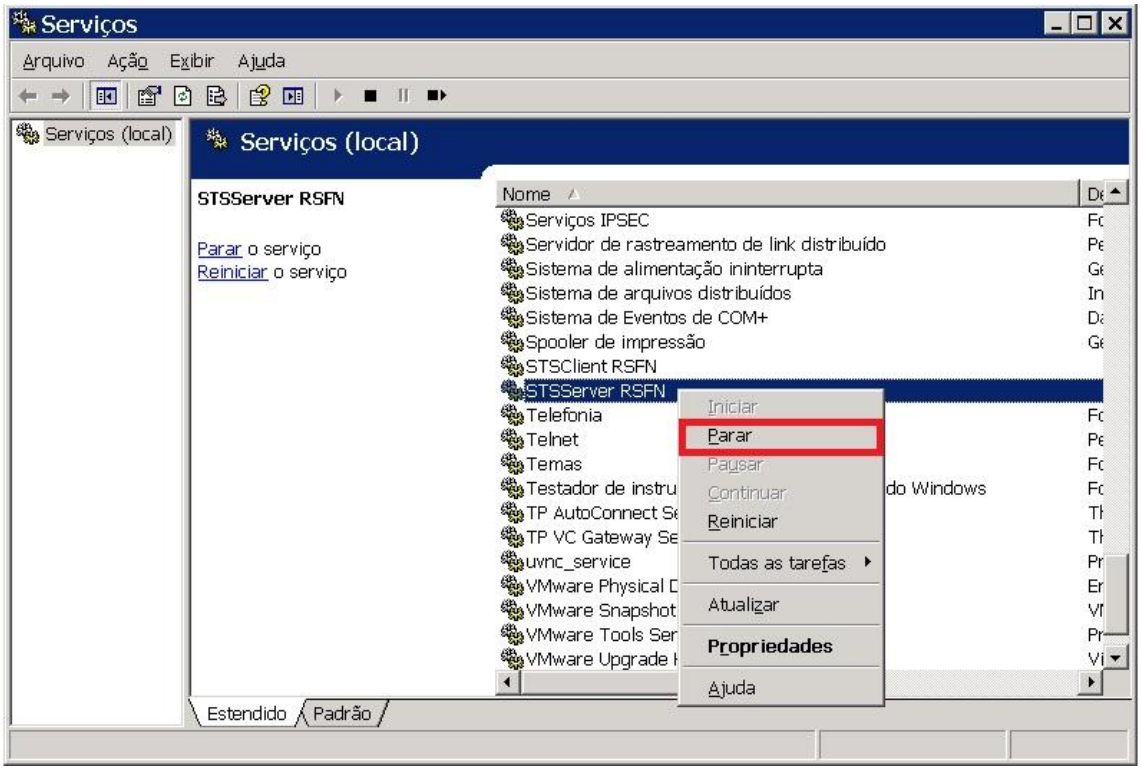
Para salvar os arquivos de eventos e certificados em diretórios remotos, há necessidade de alteração das credenciais de execução do serviço STS RSFN. Veremos a seguir como fazer para alterar essas credenciais:

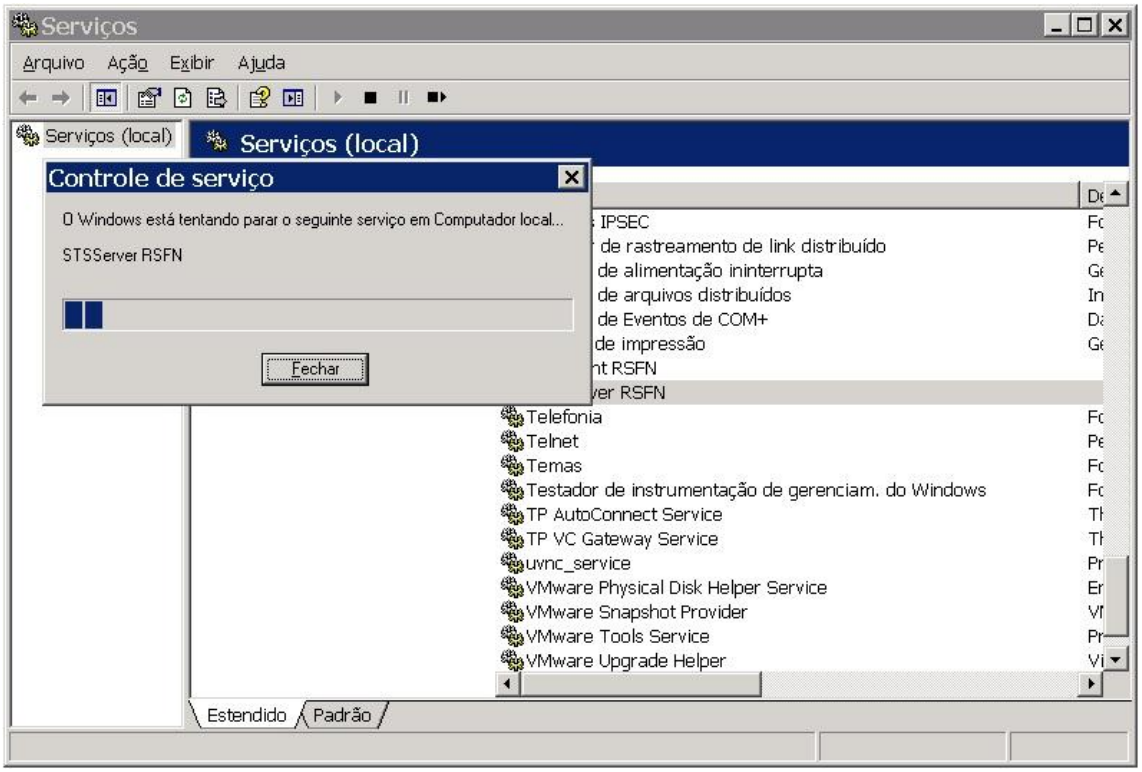
- **STSServer RSFN (PASTAS DE LOGS E CERTIFICADOS)**

a) Abra o gerenciador de serviços do Windows (**`Iniciar > Executar > services.msc`**):

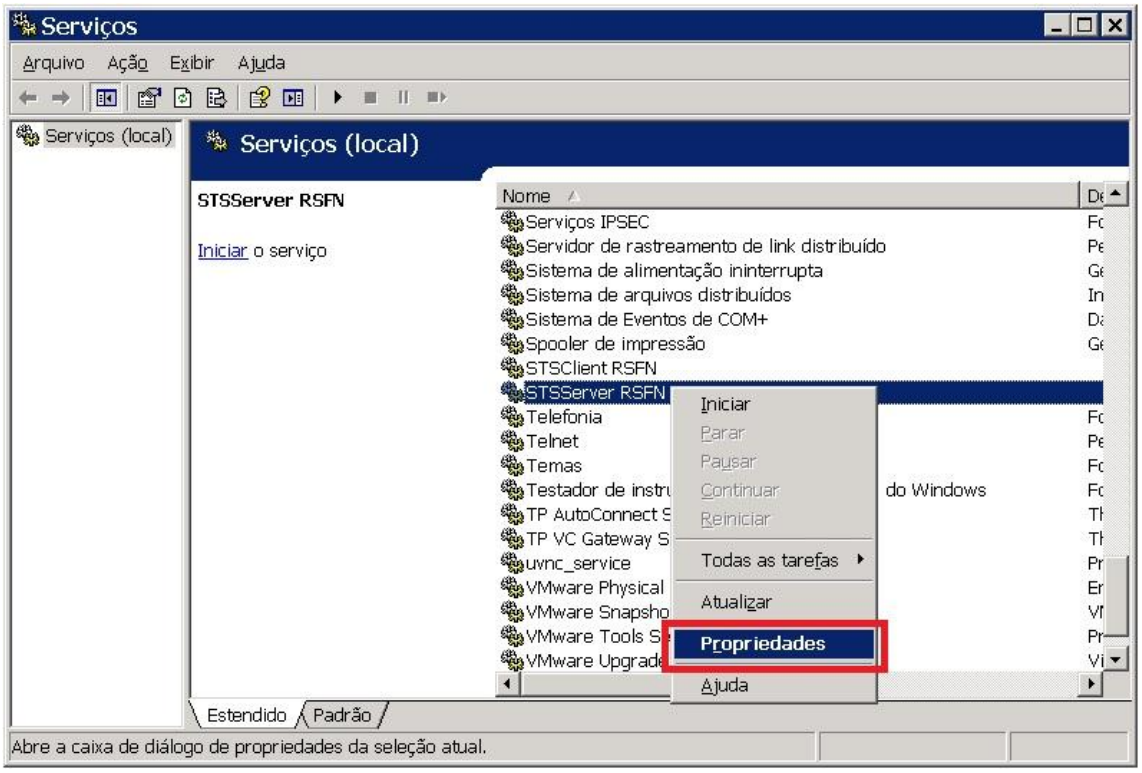


b) Localize o serviço **"STSServer RSFN"**, clique com o botão direito do mouse e pare sua execução.

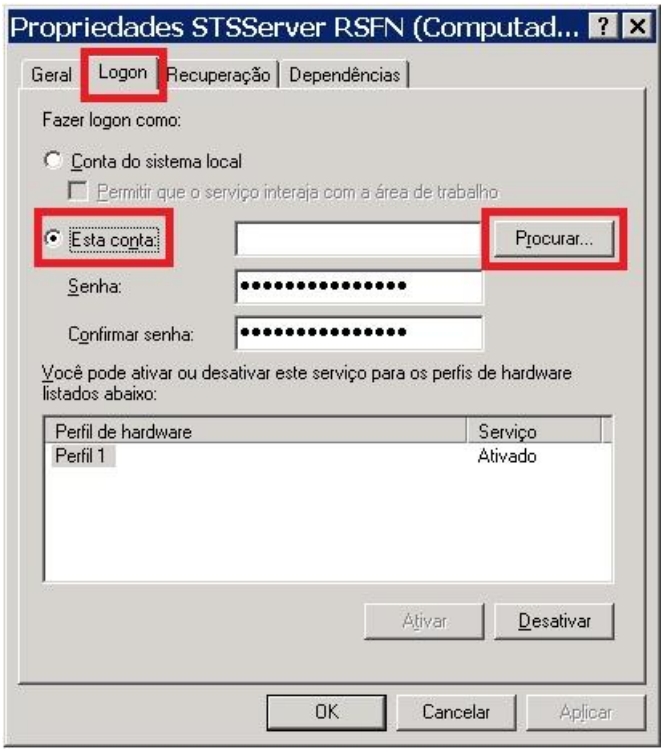




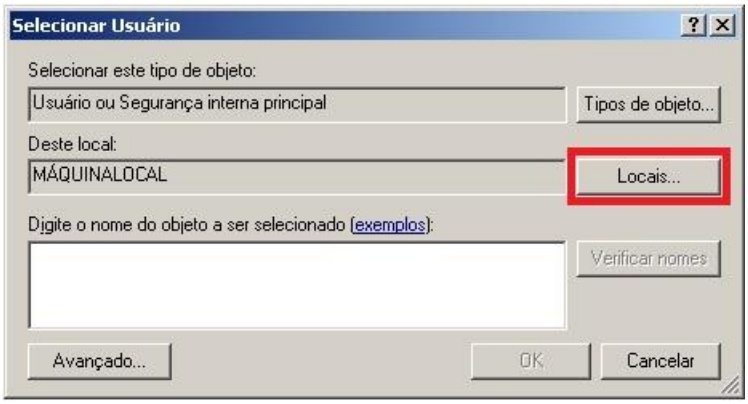
c) Clique com o botão direito do mouse sobre o serviço e selecione a opção “Propriedades” para realizar a alteração.



d) Abra a aba **"Logon"** e habilite a opção **"Esta conta:"**. Clique em **[Procurar...]** para localizar o domínio do usuário que possui as credenciais.

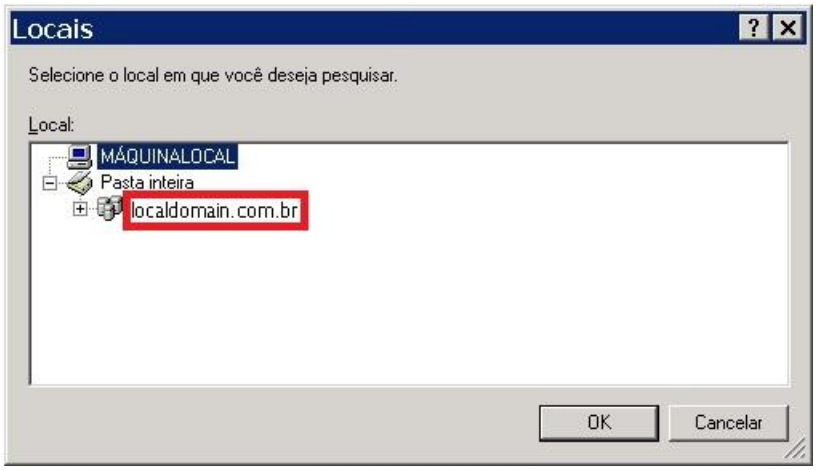


e) Clique no botão **[Locais...]** e uma nova janela será aberta.

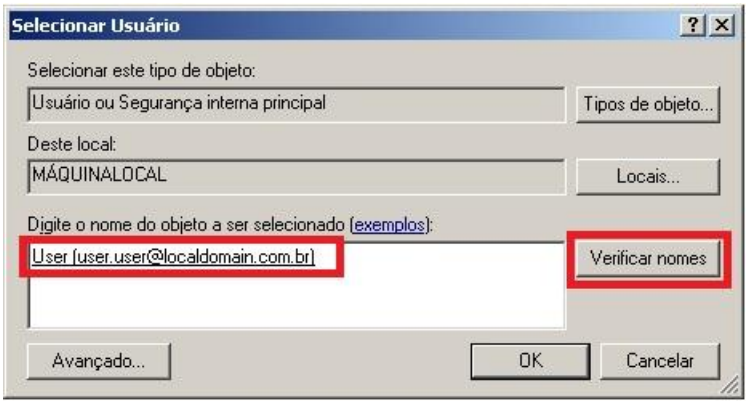


f) Insira o nome de usuário credenciado e sua respectiva senha para abrir a descoberta da rede.

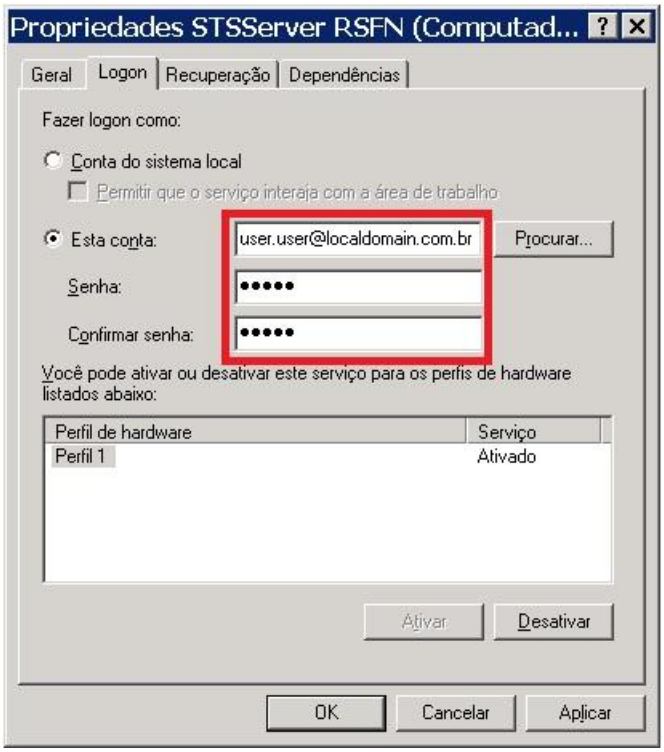
g) Selecione o domínio do qual o usuário pertence e confirme clicando no botão **[Ok].**



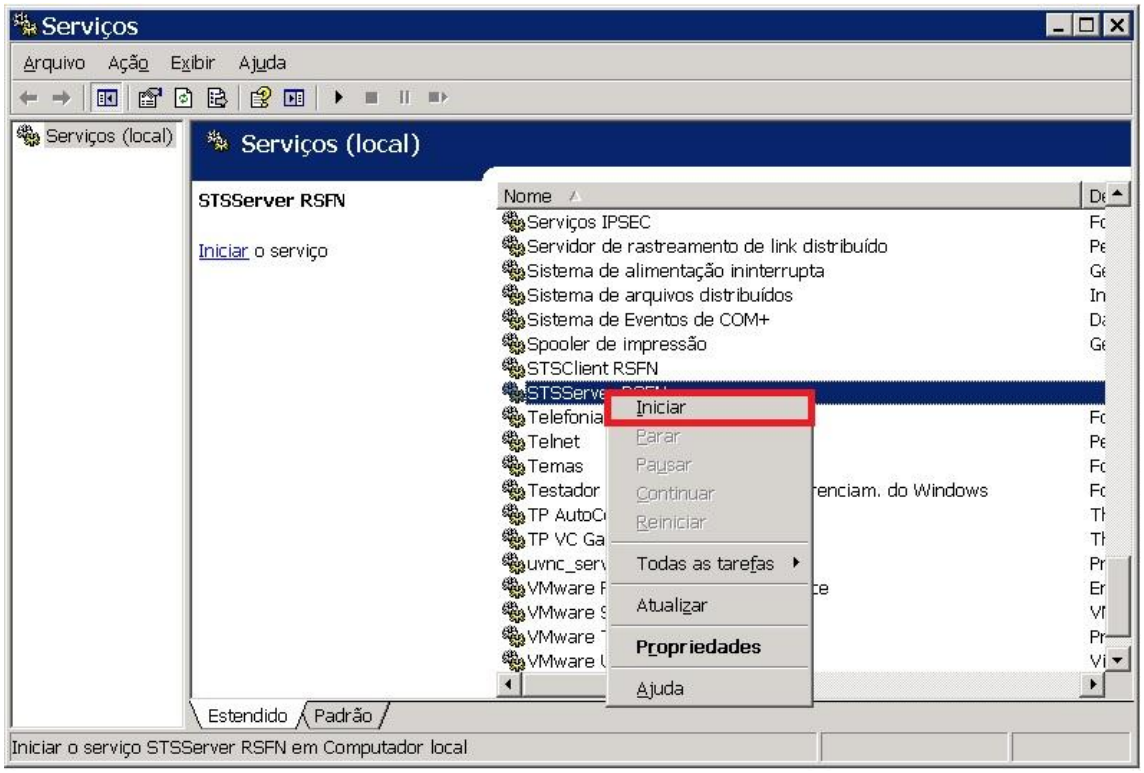
h) Entre com o nome do usuário no campo **"Digite o nome do objeto a ser selecionado (exemplos):"** e em seguida clique no botão **[Verificar nomes]** para que ele encontre o nome do usuário dentro do domínio. Clique no botão **[Ok]** para confirmar.

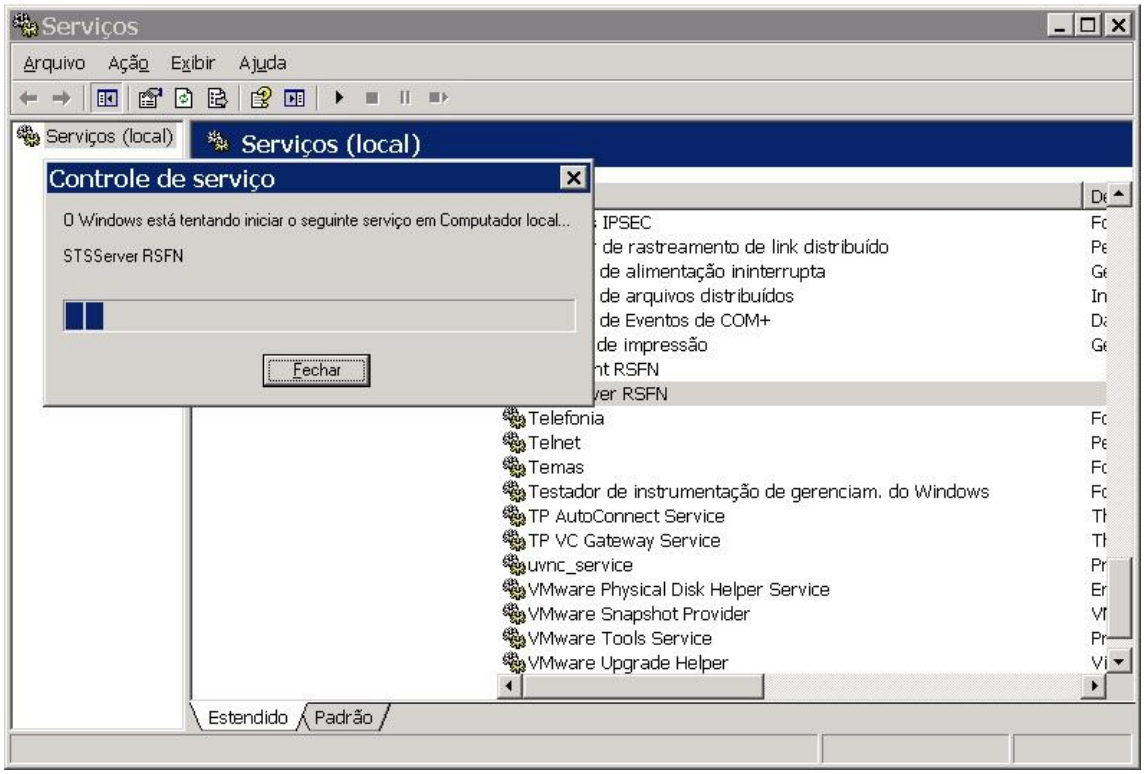


i) Confirme o nome do usuário no campo **"Esta conta:"**, digite a sua respectiva senha e confirme-a no seu devido campo.



j) Clique no botão **[Aplicar]** para que sejam salvas as alterações e em **[Ok]** para retornar a tela de lista de serviços dos Windows. Para que essas alterações sejam efetivadas, basta iniciar o serviço, clicando com o botão direito do mouse em cima do serviço **"STSServer RSFN"** e selecionando a opção **"Iniciar"**.



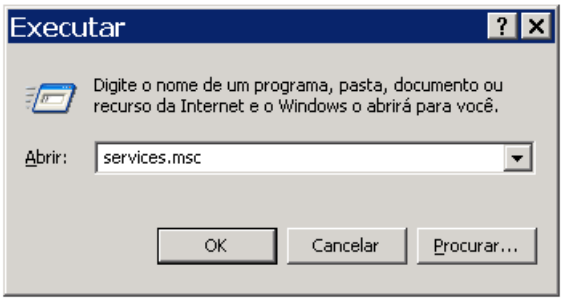


k) Após alterar a configuração de execução do serviço, pode-se utilizar um diretório remoto alterando o seu caminho na aba **"Monitoração"** e **"Certificados"** do

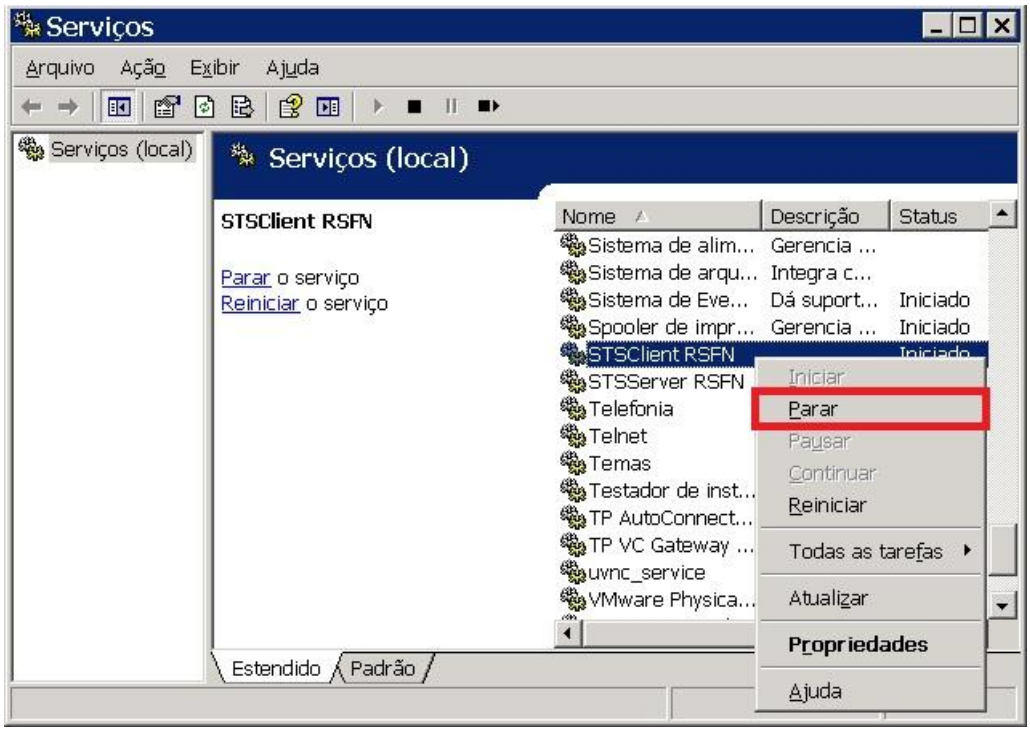
aplicativo **<Parâmetros do Servidor>**, mais informações sobre as abas e configurações podem ser encontrados nos itens **5.2.4** e **5.2.6** deste manual.

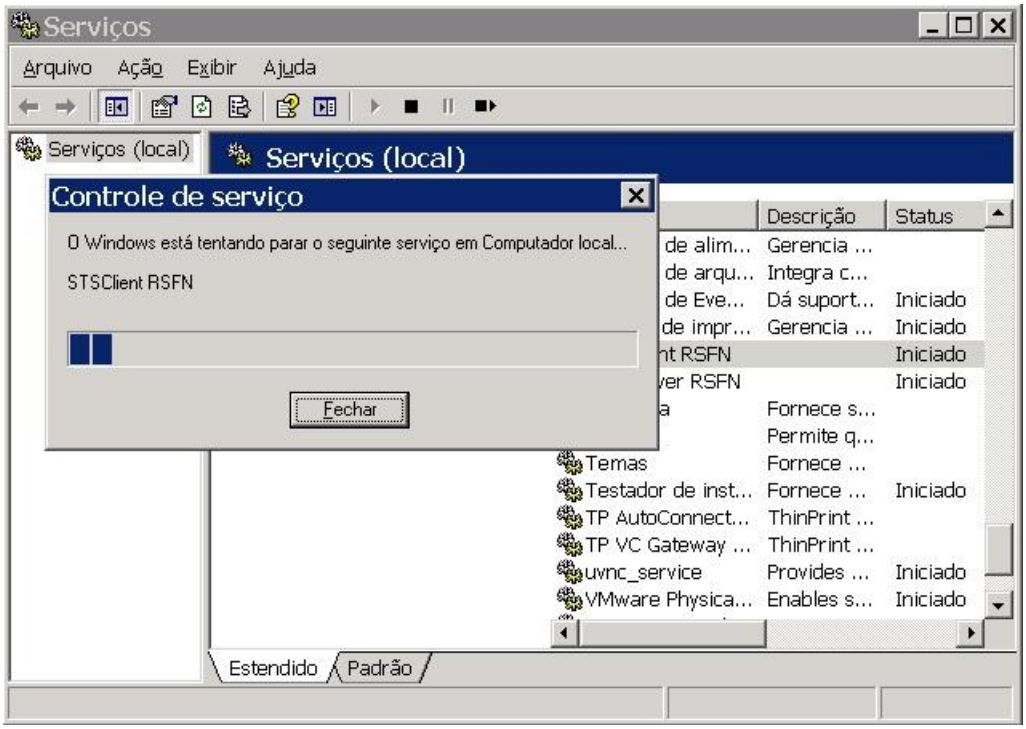
- **STSClient RSFN (LOGS)**

a) Abra o gerenciador de serviços do Windows (**`Iniciar > Executar > services.msc`**):

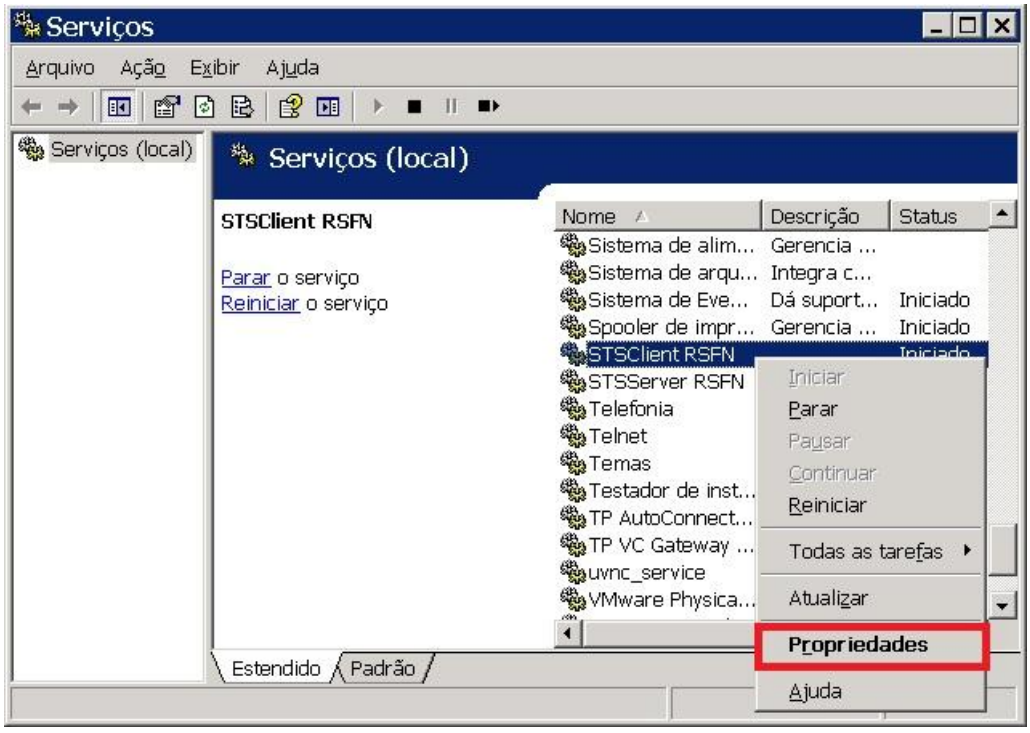


b) Localize o serviço **"STSClient RSFN"**, clique com o botão direito do mouse sobre ele e pare a sua execução.

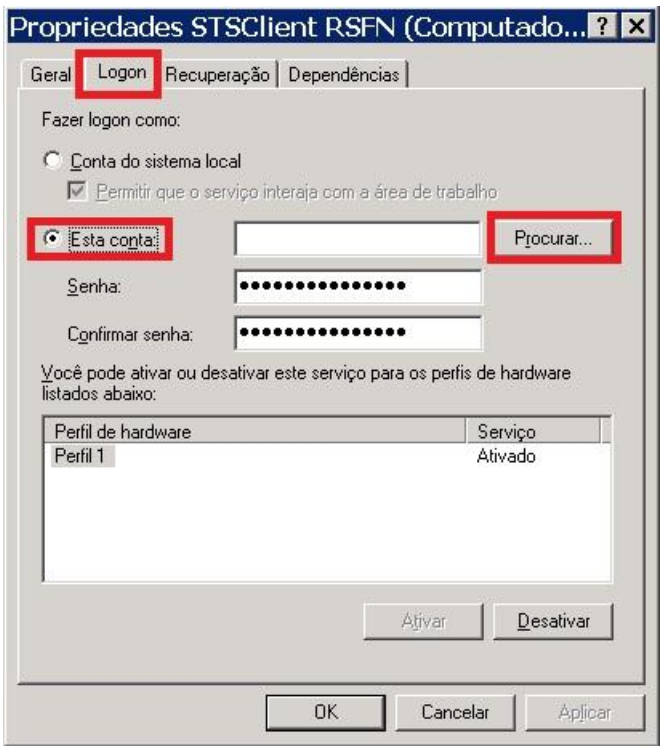




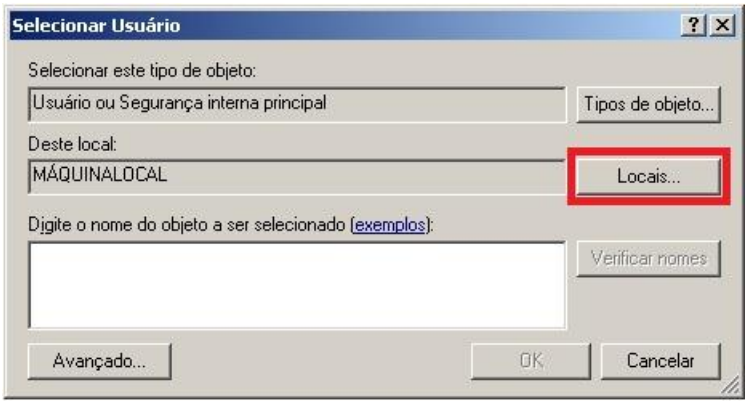
c) Clique com o botão direito do mouse e selecione a opção **"Propriedades"** para realizarmos a alteração.



d) Abra a aba **"Logon"** e habilite a opção **"Esta conta:"**. Clique em **[Procurar...]** para localizar o domínio do usuário que possui as credenciais.

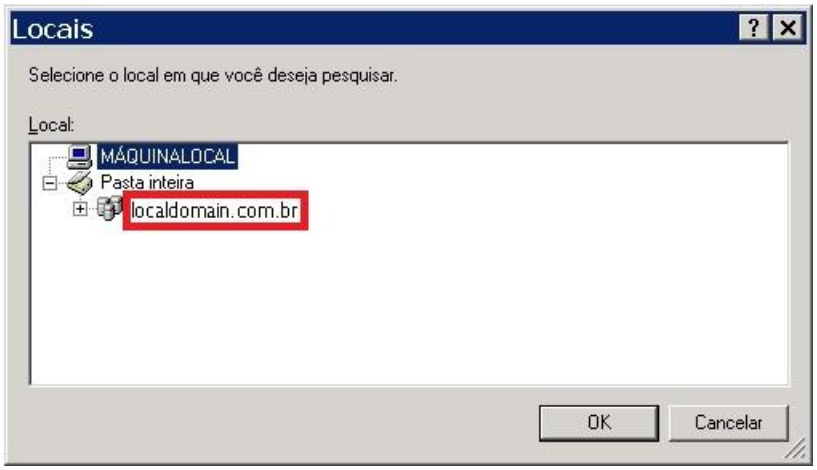


e) Clique no botão **[Locais...]** e uma nova janela será aberta.

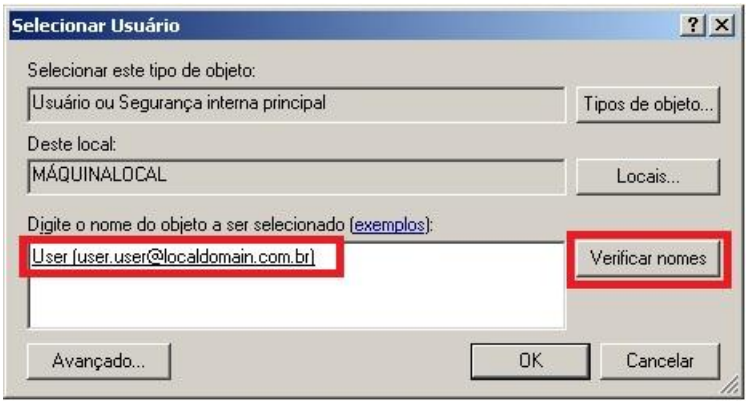


f) Insira o nome de usuário credenciado e sua respectiva senha para abrir a descoberta da rede.

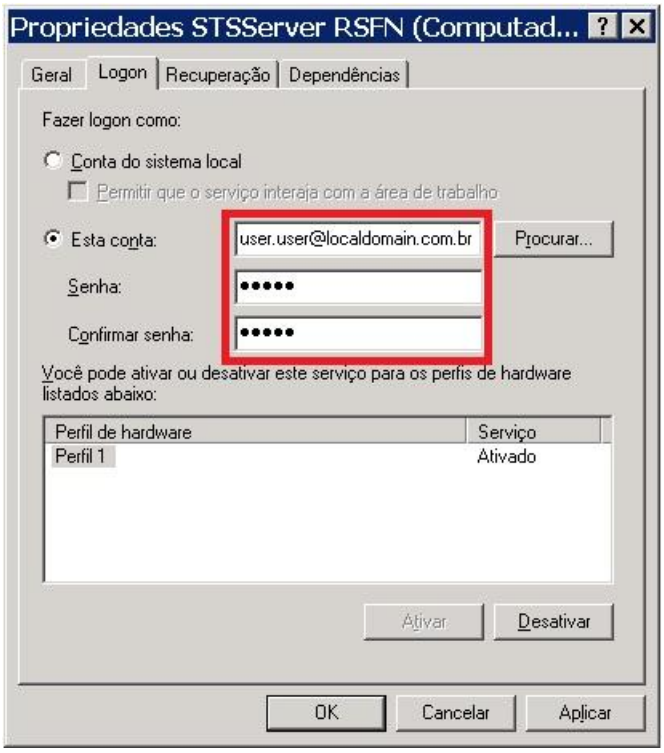
g) Selecione o domínio do qual o usuário pertence e confirme clicando no botão **[Ok].**



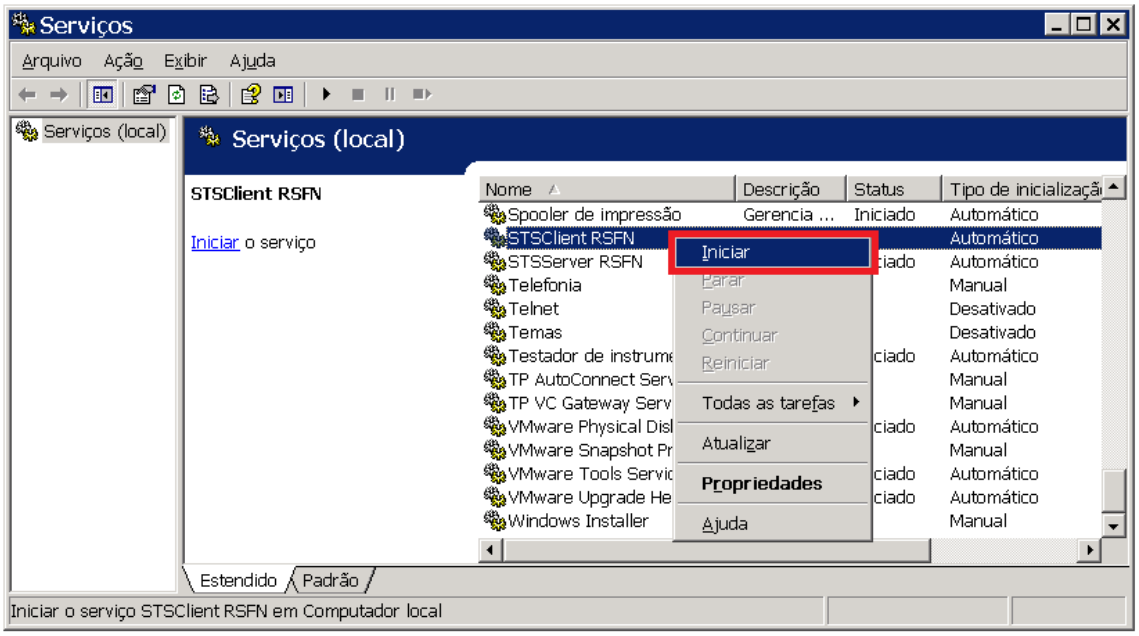
h) Entre com o nome do usuário no campo **"Digite o nome do objeto a ser selecionado (exemplos):"** e em seguida clique no botão **[Verificar nomes]** para que ele encontre o nome do usuário dentro do domínio. Clique no botão **[Ok]** para confirmar.

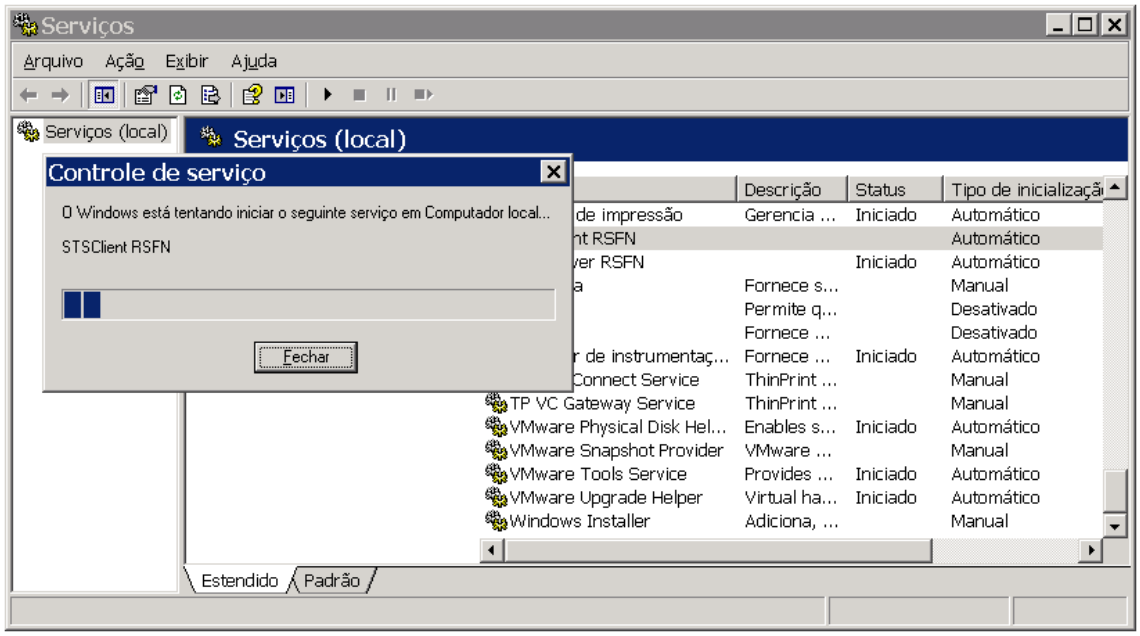


i) Confirme o nome do usuário no campo **"Esta conta:"**, e digite a sua respectiva senha e confirme-a no seu devido campo.



j) Clique no botão **[Aplicar]** para que sejam salvas as alterações e em **[Ok]** para retornar a tela de lista de serviços dos Windows. Para que essas alterações sejam efetivadas, basta iniciar o serviço, clicando com o botão direito do mouse em cima do serviço **"STSClient RSFN"** e selecionando a opção **"Iniciar"**.





k) Após realizar a alteração na configuração de execução do serviço, pode-se utilizar um diretório remoto alterando o seu caminho no quadro **"Log"** do aplicativo **<Parâmetros do Cliente>**, mais informações sobre as configurações do cliente podem ser encontradas no item **5.3** deste manual.

7 GLOSSÁRIO

AC – Sigla de Autoridade Certificadora

Alias DNS – Associação de um endereço IP/nome principal a outro nome qualquer.

CSR - *Certificate Signing Request*

1. A entidade que deseja emitir o certificado gera um par de chaves criptográficas (uma chave pública e uma chave privada).

2. Em seguida a entidade gera um arquivo chamado *Certificate Signing Request* (CSR) composto pela chave pública da entidade e mais algumas informações que a AC requer sobre a entidade e é assinado digitalmente pela chave privada da própria entidade e envia o CSR cifrado pela chave pública da AC.

3. Então é necessário o comparecimento físico de um indivíduo responsável por aquela identidade em uma Autoridade de Registro (AR) (em alguns casos a AR vai até o cliente) para confirmação dos dados contidos no CSR e se necessário o acréscimo de mais algum dado do responsável pelo certificado e emissão do certificado.

4. Finalmente o CSR é "transformado" em um certificado digital assinado pela AC e devolvido ao cliente.

DN – *Distinguished Name*. São dados da Instituição que ficam gravadas no certificado, no SPB é composta de 4 campos obrigatórios: CN, OU, O e C.

Onde:

O campo Common Name (CN) refere-se ao nome da Instituição.

O campo Organizational Unit (OU) deve ser preenchido com a ISPB e/ou o SISBACEN.

O campo Organization Name (O) com conteúdo fixo igual a “ICP-Brasil”.

O campo Country Name (C) com conteúdo fixo igual a “BR”.

Exemplo:

CN = Banco Central do Brasil

OU = 00038166

OU = 00038

O = ICP-Brasil

C = BR

Failover – Define um servidor secundário do que, se configurado, deve atender às requisições de criptografia quando o servidor primário estiver inoperante.

FAKE – Conotação de falso, inválido para uso em ambiente de produção ou homologação.

Hash – Um *hash* (ou escrutínio) é uma sequência de bits geradas por um algoritmo de dispersão, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F), representando 1/2 byte cada. O conceito teórico diz que "*hash* é a transformação de uma grande quantidade de informações em uma pequena quantidade de informações".

Essa sequência busca identificar um arquivo ou informação unicamente. Por exemplo, uma mensagem de correio eletrônico, uma senha, uma chave criptográfica ou mesmo um arquivo. É um método para transformar dados de tal forma que o resultado seja (quase) exclusivo. Além disso, funções usadas em criptografia garantem que não é possível a partir de um valor de *hash* retornar à informação original.

Como a sequência do *hash* é limitada, muitas vezes não passando de 512 bits, existem colisões (sequências iguais para dados diferentes). Quanto maior for a dificuldade de se criar colisões intencionais, melhor é o algoritmo.

Uma função de *hash* recebe um valor de um determinado tipo e retorna um código para ele. Enquanto o ideal seria gerar identificadores únicos para os valores de entrada, isso normalmente não é possível: na maioria dos casos, o contra-domínio de nossa função é muito menor do que o seu domínio, ou seja, x (o tipo de entrada) pode assumir uma gama muito maior de valores do que (o resultado da função de *hash*).

Header – Cabeçalho de uma mensagem qualquer que passa pelo processo de criptografia, seus padrões são estabelecidos de acordo com o Manual de Segurança da RSFN ou da CIP.

HSM (*Hardware Security Module*) – É um tipo de processador criptográfico que tem por principal função proteger as chaves de criptografia. Dependendo do algoritmo de criptografia utilizado em operações criptográficas, ele também funciona como acelerador de operações.

ICMP (*Internet Control Message Protocol*) – sigla para o inglês *Internet Control Message Protocol*, é um protocolo integrante do Protocolo IP, definido pelo RFC 792, e utilizado para fornecer relatórios de erros à fonte original. Qualquer computador que utilize IP precisa aceitar as mensagens ICMP e alterar o seu comportamento de acordo com o erro relatado. Os gateways devem estar programados para enviar mensagens ICMP quando receberem datagramas que provoquem algum erro.

As mensagens ICMP geralmente são enviadas automaticamente em uma das seguintes situações:

- Um pacote IP não consegue chegar ao seu destino (i.e. Tempo de vida do pacote expirado)
- O Gateway não consegue retransmitir os pacotes na frequência adequada (i.e. Gateway congestionado)
- O Roteador ou Encaminhador indica uma rota melhor para a máquina a enviar pacotes.

Ferramentas comumente usadas em Windows baseadas nesse protocolo são: Ping e Traceroute.

Alguns firewalls, geralmente instalados em servidores Windows ou Unix, bloqueiam as respostas (ICMP Reply), dificultando o Ping e o Traceroute (tracert). Isto por diversas razões. Uma delas é para bloquear os ataques de hackers, que consiste na sobrecarga da memória,

enviando dados (em ping) até o sistema não ter a capacidade de administrar suas próprias funções.

IF – Sigla de Instituição Financeira.

ISPB – Sigla de Instituição do Sistema de Pagamentos Brasileiro.

Legado - Refere-se ao sistema que já vem sendo usado na empresa.

Load Balance (Balanceamento de carga) – Em rede de computadores, o balanceamento de carga é uma técnica para distribuir a carga de trabalho entre dois ou mais computadores, enlaces de rede, UCPs, discos rígidos ou outros recursos, a fim de otimizar a utilização de recursos, maximizar o desempenho, minimizar o tempo de resposta e evitar sobrecarga. Utilizando múltiplos componentes com o balanceamento de carga, em vez de um único componente, pode aumentar a confiabilidade através da redundância.

LOG – registro de eventos em um sistema de computadores.

Mensageria - Refere-se ao sistema cliente do STS RSFN, responsável por preparar as mensagens, ou arquivos, que serão transmitidos para outras instituições. Após preparar a mensagem, ou arquivo, este sistema deve solicitar ao STS RSFN que realize as funções de criptografia requeridas pelo protocolo de segurança.

PIN – Sigla de *Personal Identification Number*. Refere-se ao Número de Identificação Pessoal, popularmente conhecido como “senha”.

PING – Comando utilizado na janela de *prompt* de comando para verificação de conectividade entre computadores/equipamentos/dispositivos.

RSA 1024 – Refere-se a um algoritmo de criptografia que utiliza uma chave RSA de 1024 bits.

RSA 2048 – Refere-se a um algoritmo de criptografia que utiliza uma chave RSA de 2048 bits.

SHA-1 – Sigla de *Secure Hash Algorithm*. Algoritmo de hash utilizado para autenticar criptogramas gerados com chaves RSA de 1024 bits.

SHA-256 - Sigla de *Secure Hash Algorithm*. Algoritmo de hash utilizado para autenticar criptogramas gerados com chaves RSA de 2048 bits.

SNMP – O protocolo SNMP (do inglês *Simple Network Management Protocol* - Protocolo Simples de Gerência de Rede) é um protocolo de gerência típica de redes UDP, da camada de aplicação, que facilita o intercâmbio de informação entre os dispositivos de rede, como placas e comutadores (em inglês: switches). O SNMP possibilita aos administradores de rede gerenciar

o desempenho da rede, encontrar e resolver seus eventuais problemas, e fornecer informações para o planejamento de sua expansão, dentre outras.

Standby – Refere-se ao modo de espera. Normalmente servidores de **Failover**, quando não estão operando, ficam no estado **standby**.

TCP Socket – Especificamente em computação, um socket pode ser usado em ligações de redes de computadores para um fim de um elo bidirecional de comunicação entre dois programas. A interface padronizada de sockets surgiu originalmente no sistema operacional Unix BSD (*Berkeley Software Distribution*); portanto, eles são muitas vezes chamados de Berkeley Sockets. É também uma abstração computacional que mapeia diretamente a uma porta de transporte (TCP ou UDP) e mais um endereço de rede. Com esse conceito, é possível identificar unicamente um aplicativo ou servidor na rede de comunicação IP.

Thread – é uma forma de um processo dividir a si mesmo em duas ou mais tarefas que podem ser executadas concorrentemente. O suporte à *thread* é fornecido pelo próprio sistema operativo (SO), no caso da linha de execução ao nível do núcleo (em inglês: *Kernel-Level Thread* (KLT)), ou implementada através de uma biblioteca de uma determinada linguagem, no caso de uma *User-Level Thread* (ULT).

Uma *thread* permite, por exemplo, que o utilizador de um programa utilize uma funcionalidade do ambiente enquanto outras linhas de execução realizam outros cálculos e operações.

Token – Refere-se a um hardware capaz de gerar e armazenar chaves de criptografia e outras informações sensíveis.

UNC – Sigla de convenção de nomenclatura universal. É uma sintaxe que pode descrever a localização de um arquivo, componente ou pasta compartilhada.