CONFIGURAÇÃO GLASSFISH – SSL

(CLIENTE NÃO POSSUI CERTIFICADO)

INFORMAÇÕES

Este manual tem por finalidade auxiliar na aquisição do certificado digital, importação do certificado, configuração do domínio glassfish e aplicações Senior, para serem acessadas de modo seguro com HTTPS.

REQUISITOS

- Ter um domínio do glassfish já configurado;

- Acesso ao servidor com usuário administrador;

- Aplicativo Portecle. Link: http://portecle.sourceforge.net/

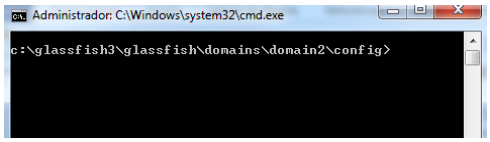
PROCEDIMENTO

1 Aquisição do certificado digital

Para comprar um certificado digital para acesso seguro no glassfish, é necessário acionar uma Autoridade certificadora (Digicert, Certisign, Geotrust, etc...) e encaminhar a ela, um arquivo com as informações do certificado a ser emitido. Abaixo, o procedimento para gerar este arquivo:

1.1 – Gerar arquivo .CSR (Certificate Signing Request)

1.1.1 Abra o CMD (Prompt de comando) e acesse o seguinte diretório:
[Diretório do domínio]\config



1.1.2 Digite o seguinte comando:
keytool -genkey -keyalg RSA -alias [alias] -keystore keystore.jks -keysize 2048
[alias] deve ser substituído por um nome da sua preferencia (Exemplo: **seniorssl**)
Este nome que será usado no "alias" deve ser anotado, pois será utilizado mais adiante.

1.1.3 Será solicitada a senha da Keystore. Digite a senha padrão: **changeit**

1.1.4 Serão solicitadas algumas informações ref. Ao certificado. Seguem exemplos:
what is your first and last name?
- Neste item, digite o CN (nome comum) que será utilizado para o acesso HTTPS.
  Exemplo: **seniorssl.senior.com.br**

what is the name of your organizational unit?
- Neste item, costuma-se ser informado o nome da empresa simplificado. Exemplo: **Senior**

what is the name or your organization?
- Neste item, digite o nome da empresa completo. Exemplo: **Senior Sistemas**

what is the name of your city ou locality?
- Neste item, informe o nome da cidade. Exemplo: **Blumenau**

what is the name of your state or province?
- Neste item, digite o nome do Estado. Exemplo: **Santa Catarina**

what is the two-letter country code for this unit?
- Neste item, informe as duas letras do seu país. Exemplo: **BR**

1.1.5 Será solicitada uma senha. Digite a mesma senha da keystore: **changeit**

1.1.6 Mantenha o prompt de comando aberto e digite o comando seguido de ENTER:

keytool -certreq -keyalg RSA -alias [alias] -file filename.csr -keystore keystore.jks
[alias]: deve ser substituído pelo mesmo alias utilizado no passo **1.1.2**
Filename.csr: deve ser informado um nome para arquivo que será gerado. Manter a extensão **.csr**

1.1.7 Será gerado no diretório **config** do domínio um arquivo com o nome informado no passo anterior.

1.2 – Adquirir certificado junto a CA (Certification Authority)

Entre em contato com a autoridade certificadora da sua escolha (Digicert, Certisign, Geotrust, etc...), e efetue a compra do certificado digital.

Deve ser enviado para a autoridade certificadora, o arquivo **.CSR** que foi gerado no passo 1.1.

Caso o cliente já tiver um certificado digital emitido e sendo utilizado em outras aplicações (IIS, Apache, etc...), pode ser efetuada a remissão do mesmo certificado junto à autoridade certificadora para ser utilizado no Glassfish. A maioria das autoridades certificadoras faz esse procedimento sem custo adicional, inclusive algumas possuem um portal para o próprio cliente efetuar a remissão.

Exemplo de portal para remissão:

https://knowledge.geotrust.com/support/knowledge-base/index?page=content&id=SO5989

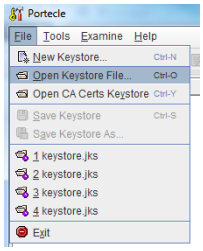
2 Importar Certificado enviado pela autoridade certificadora

2.1 Certifique-se de que o certificado digital enviado pela autoridade certificadora contenha toda a cadeia de certificação e salve o certificado digital em algum lugar no servidor. Iremos utilizar mais a frente.

Dica (opcional): Importe o certificado digital no Windows (MMC > Certificados) para verificar se a cadeia de certificados é exibida corretamente. Se preferir, após importar no Windows, exporte-a novamente incluindo a cadeia de certificados completa. Salve novamente este arquivo e utilize este para importar no glassfish (Mais a frente).

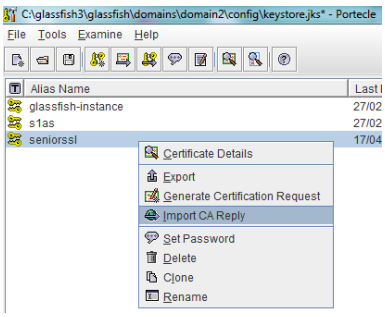
2.2 Faça um backup do arquivo **keystore.jks** original que se encontra no ***[diretório_do_dominio]\config\keystore.jks***

2.3 Abra o aplicativo **portecle** e clique em File > Open Keystore File

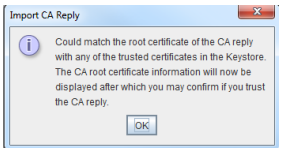


2.4 Abra o arquivo **keystore.jks** que se encontra no ***[diretório do dominio]\config\keystore.jks***

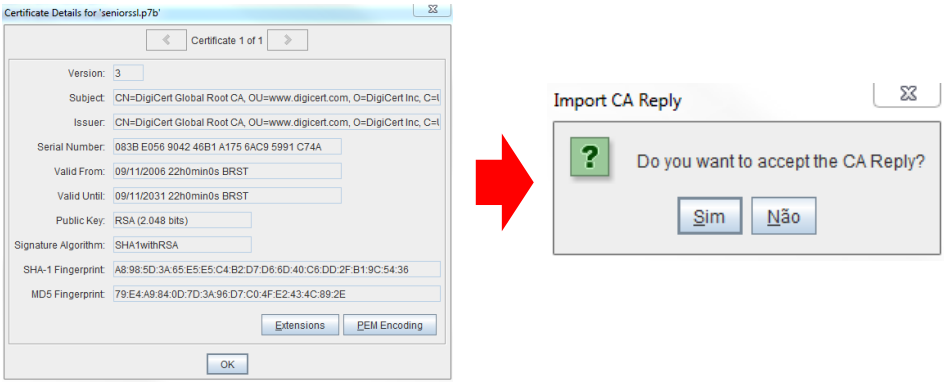
2.5 Clique com o botão direito sobre a chave que possui o ALIAS que foi gerado no passo 1.1.2 em seguida clique em **Import CA Reply**



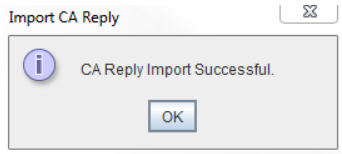
2.6 Abra o arquivo do certificado salvo no item 2.1. A tela abaixo aparecerá, clique em OK.



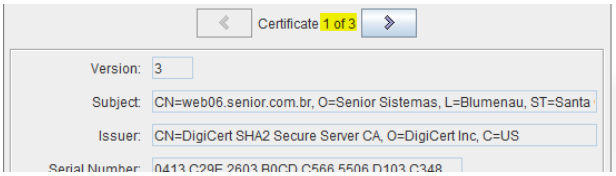
2.7 A tela abaixo aparecerá, clique em **OK**, e na próxima, clique em **SIM**.



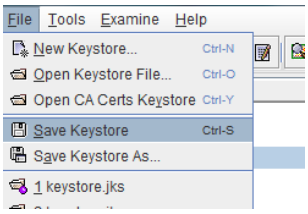
2.8 Será solicitada a senha da chave. Digite **changeit** e clique em **OK**.
A tela abaixo será apresentada informando que a importação foi efetuada com sucesso.



2.9 Dê duplo clique sobre a chave **seniorssl** e verifique se a cadeia de certificados está correta. No nosso exemplo, são 3 certificados no total. Se a cadeia não aparecer, o acesso seguro não funcionará.



2.10 Clique em **File > Save KeyStore** para salvar as alterações efetuadas no arquivo keystore.jks.

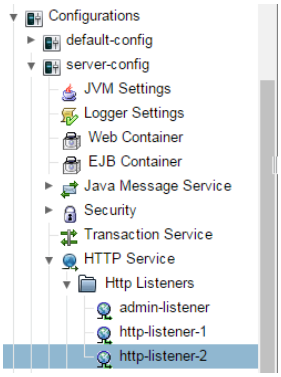


IMPORTANTE!!

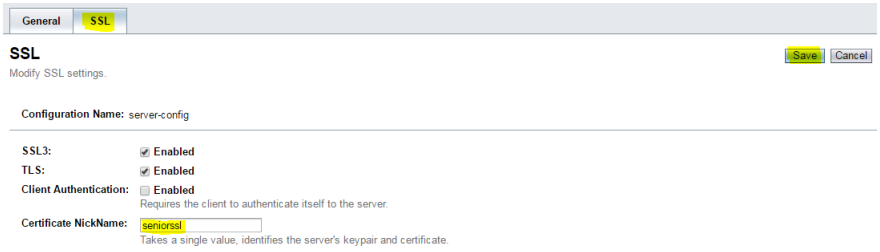
Terminado este passo, faça um novo backup do arquivo **Keystore.jks** e nomeie este backup informando que possui o certificado importado. Este arquivo é essencial para utilizar SSL em outro domínio Glassfish, ou, caso ocorra algum incidente que necessite reinstalar o glassfish.

3 Configurar Domínio do Glassfish

3.1 Acesse a ***interface de gerenciamento do domínio glassfish > Configurations > server-config > HTTP Service > Http Listeners > http-listener-2***;



3.2 Clique na aba **SSL** e altere o campo **Certificate NickName** para o nome da chave que contem o alias criado no item 1.1.2, salve e reinicie o domínio do glassfish.



3.3 Após iniciar o domínio, faça um teste de acesso HTTPS da seguinte forma:
https://[CN item1.1.4]:[porta do http-listener-2]
Este acesso deverá abrir a página do Glassfish com o certificado validado.

OBS.: Esta URL de acesso deve estar de acordo com a URL informada no item 1.1.4. Caso contrário, o acesso não validará o certificado.

4 Configuração das aplicações Senior

4.1 Se for uma instalação nova, e não houver nenhuma aplicação “deployada” no domínio Glassfish, rode o SeniorInstaller.exe e quando solicitado, informe o domínio do glassfish já com a URL HTTPS, conforme teste realizado no item 3.3.

4.2 Se o domínio do Glassfish já possuir aplicações deployadas, altere as URLs de acesso às aplicações dentro do SeniorConfigCenter.exe informando a URL com HTTPS conforme teste realizado no item 3.3.
OBS.: Para WebServices, altere a URL no SeniorConfigCenter.exe, e refaça o deploy acessando o SeniorDeployTool utilizando a URL HTTPS (item 3.3).

Talvez algumas aplicações não funcionem corretamente após esse procedimento. Nesses casos, sugerimos rodar o SeniorInstaller para refazer os deploys informando a nova URL.

FIM DO PROCEDIMENTO