LINUX - TOMCAT – KEYTOOL – INSTALAR CERTIFICADO_V2

1 - Após fazer a emissão/download do Arquivo de certificado a partir do e-mail recebido
Exportar o arquivo ".CER" para o "modo X.509" (conforme Instruções)

Após...

2 - Fazer a importação dos certificados:
AC_PRODEMGE_G3.cer, AC_CERTISIGN_G6.cer, ICP_BRASIL_V2.cer e o certificado original.
- Copie os Arquivos (AC_PRODEMGE_G3.cer, AC_CERTISIGN_G6.cer, ICP_BRASIL_V2.cer, certificado.cer, www.site.com.br.cer) para o Diretório “Keys”
Obs:
- Os certificados estão disponíveis para download no site
- O arquivo “certificado.cer” é o certificado original que você fez download do link recebido por e-mail
- O arquivo “www.site.com.br.cer” é o arquivo exportado para “modo X.509”

2.1 - Siga os comandos abaixo, para fazer a importação...

- **Importação da Cadeia AC_PRODEMGE**
keytool -import -alias prodemge -keystore tomcat.key -trustcacerts -file AC_PRODEMGE_G3.cer
Enter keystore password: xxxx
Certificate reply was installed in keystore

- **Importação da Cadeia AC_CERTISIGN**
keytool -import -alias certisign -keystore tomcat.key -trustcacerts -file AC_CERTISIGN_G6.cer
Enter keystore password: xxxx
Certificate reply was installed in keystore

- **Importação da Cadeia AC_RAIZ**
keytool -import -alias raiz -keystore tomcat.key -trustcacerts -file ICP_BRASIL_V2.cer
Enter keystore password: xxxx
Certificate reply was installed in keystore

- **Importação da Certificado Original**
keytool -import -alias tomcat -keystore tomcat.key -trustcacerts -file www.site.com.br.cer
Enter keystore password: xxxx
Certificate reply was installed in keystore

---

3 – Modificar a configuração do Tomcat
Arquivo: SERVER.XML

Obs: Antes das alterações, para sua segurança, faça um backup do Arquivo “server.xml” para manter a copia original, caso houver necessidade de voltar ao formato original.

Procurar a Diretiva Æ Connector on port 8080
Modificar conforme abaixo:

<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8080 -->

<Connector URIEncoding="UTF-8" acceptCount="100" connectionTimeout="20000" debug="0" disableUploadTimeout="true" enableLookups="false" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" port="80" redirectPort="443" />

Procurar a Diretiva Æ Connector on port 8443
Modificar conforme abaixo:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector port="443"
        URIEncoding="UTF-8" maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
        enableLookups="false" disableUploadTimeout="true"
        acceptCount="100" debug="0" scheme="https" secure="true"
        clientAuth="false" sslProtocol="TLS"
        keystoreFile="/etc/httpd/ssl/tomcat.key"
        keystorePass="site" />
```

4 – Executar os Serviços
STOP no Tomcat
START no Tomcat

5 – Teste no browser
– Acesse a URL do site
– Aparecerá o cadeado
– Conferir a data de validade e o caminho da certificação