UNIVERSIDADE REGIONAL DE BLUMENAU
CENTRO DE CIÊNCIAS EXATAS E NATURAIS
DEPARTAMENTO DE SISTEMAS E COMPUTAÇÃO
PROFESSOR GILVAN JUSTINO
DESENVOLVIMENTO DE SISTEMAS SEGUROS

Lista de Exercícios 12

Publique as saídas apresentadas pelo navegador nas três questões abaixo. Anexe as respostas às perguntas colocadas nas questões 1 e 2.

Questão 1

1) Utilize a ferramenta KeyStore Explorer e crie um repositório no formato JKS. Adicione dois certificados como descrito abaixo:
   a) Um certificado indicando que se trata de uma "unidade certificadora" (na extensão "Basic constraint" indique que o sujeito é uma AC).
   b) Utilize o certificado anterior para criar um novo certificado. Este será o certificado do servidor.

2) Instale o servidor de páginas *Tomcat* (http://tomcat.apache.org/) e ative a configuração para TLS, como descrito:
   a) Veja em: `https://dzone.com/articles/setting-ssl-tomcat-5-minutes`, na sessão "2 – *Configuring Tomcat for using the keystore file – SSL config*" como fazer a configuração. Leve em consideração as seguintes observações:
      - O parâmetro `keystoreFile` deve conter o caminho do repositório de chaves que você criou.
      - O parâmetro `keystorePass` deve conter a chave que você criou **para o repositório**.
      - Acrescente também o atributo `keyAlias="aliasCriadoNoPassoB"` na tag `Connector`
      - Perceba que a tag `SSLHostConfig` é removida.

3) Exporte o certificado da "unidade certificadora" (criado no item "a" acima), usando o formato de texto plano PEM (que gera um arquivo com extensão.cer).

4) Através do navegador, acesse: `https://localhost:8443.`

O que acontece?

Observe os detalhes da informação apresentada. Clique sobre o código que surgir e veja a sessão *PEM encoded chain*. Confira com os certificados da keystore.

Questão 2

Importe o certificado que você exportou no item anterior, para o sistema operacional ou para o repositório utilizado pelo navegador.

- Para Windows, veja este tutorial: `https://www.thewindowsclub.com/manage-trusted-root-certificates-windows`
- Se o navegador for Firefox, utilize este tutorial: `https://origin-symwisedownload.symantec.com/resources/webguides/sslv/sslva_first_steps/Content/Topics/Configure/ssl_firefox_cert.htm`.

Tente acessar a página pelo navegador.
O que acontece?

Questão 3

Edite o certificado criado no item (b) da questão 1. Adicione a extensão "Subject alternative name" e adicione um nome alternativo, do tipo "DNS name" para o sujeito do certificado. Utilize o nome "localhost", já que estamos acessando deste local.
Tente acessar a página pelo navegador.

O que acontece?