证书文件生成方法的配置

iNode 802.1X Portal 何颖 2013-04-23 发表

证书文件生成方法的配置

一、 组网需求：

在证书认证等应用场景中需要使用服务器证书、客户端证书及根证书。本文将介绍证书的制作方法。

二、 组网图：

无

三、 配置步骤：

服务器身份验证证书的生成

1、证书服务器主页面

利用Windows自带的证书服务器，在IE地址栏中输入证书服务器的IP地址，如：http://192.168.0.109/certsrv，进入Microsoft 证书服务页面：

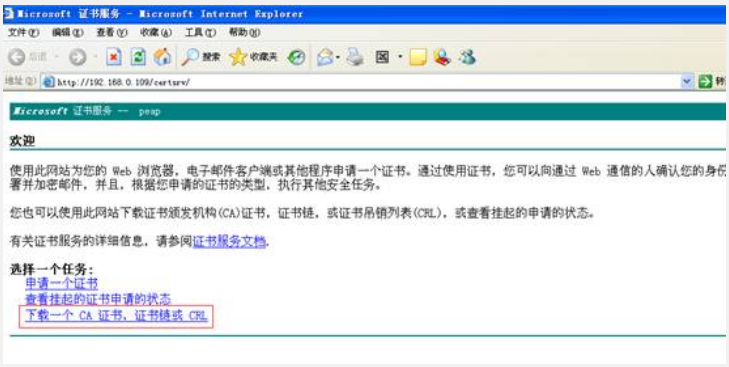

图1 Windows自带的证书服务器示意图

2、下载根证书

首先选择【下载一个CA证书，证书链或CRL】，编码方法：Base 64。

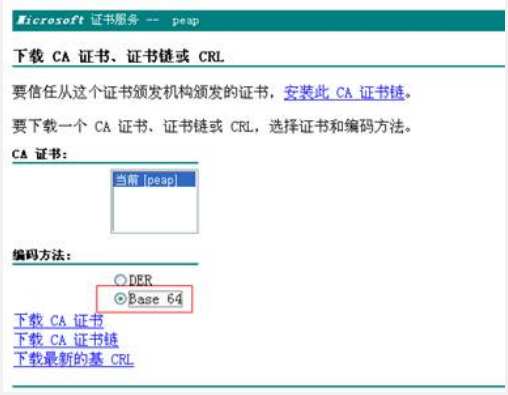

图2 下载CA证书示意图

可以点击【安装此CA证书链】，就会把根证书安装到控制台中的受信任的根证书颁发机构。

如果点击【下载CA证书】，就会下载一certnew的文件。然后再手工添加到控制台中的受信任的根证书颁发机构。

3、生成服务器身份验证证书

图3-a 下载服务器身份验证证书示意图a

1） 选择【申请一个证书】：

图3-b 下载服务器身份验证证书示意图b

2） 选择【高级证书申请】：

图3-c 下载服务器身份验证证书示意图c

3） 选择【创建并向此CA提交一个申请】：

图3-d 下载服务器身份验证证书示意图d

4） 点击【提交】，弹出一提示框： 点击【是】

图3-e 下载服务器身份验证证书示意图e

图3-f 下载服务器身份验证证书示意图f

5) 点击【安装此证书】，证书就会被安装到控制台中，如下图所示：

图3-g 下载服务器身份验证证书示意图g

6) 导出生成的服务器验证证书，右键证书文件，选择“所有任务”的“导出”。

图4-a 导出生成的服务器验证证书示意图a

7) 点击【下一步】，选择导出私钥。

图4-b 导出生成的服务器验证证书示意图b

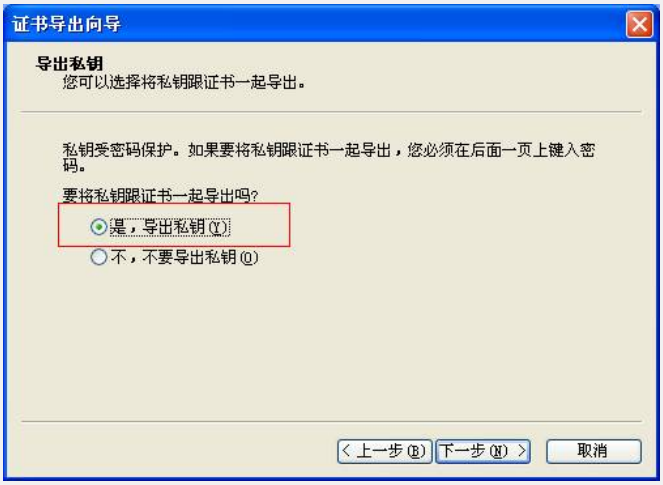

图4-c 导出生成的服务器验证证书示意图c

8) 点击【下一步】:

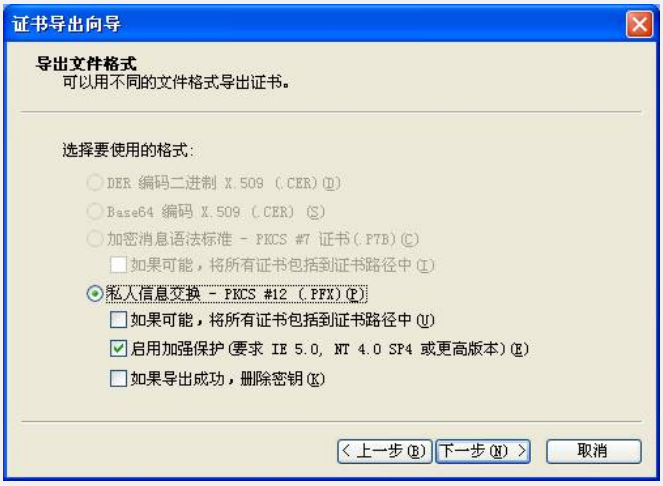

图4-d 导出生成的服务器验证证书示意图d

9) 点击【下一步】，输入导出密码。

图4-e 导出生成的服务器验证证书示意图e

10) 点击【下一步】，输入服务器证书文件存在的位置

图4-f 导出生成的服务器验证证书示意图f

11) 点击【下一步】。

图4-g 导出生成的服务器验证证书示意图g

12) 点击【完成】。查看E盘根目录：heserver.pfx 导出成功，如下图所示

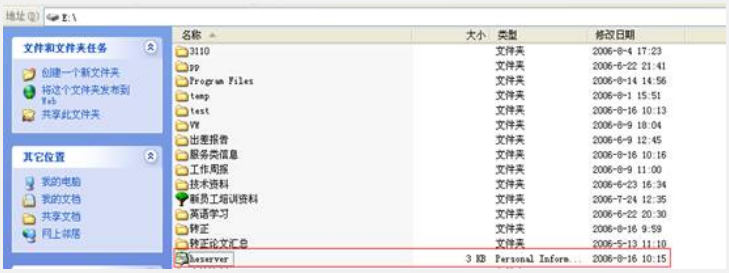

图5 导出生成的服务器验证证书完成后示意图

4. 客户端身份验证证书的生成

操作步骤和生成服务器身份验证证书的类似，只是在“高级证书申请”中，选择“客户端身份验证证书”。如图10所示：

图10 生成的客户端验证证书示意图

当证书安装完成后，在控制台可以看到该证书。如图11所示。

图11 导出生成的客户端验证证书完成后示意图

四、 配置关键点：

1） 在服务器端配置的根证书是用来签发客户端证书的根证书，而在客户端配置根证书是用来签发服务器证书的，如果服务器证书和客户端证书为同一个根证书签发的，那么服务器和客户端配置的根证书应该是一样的。

2） 注意证书的有效期。可以调整证书有效期为一个较长时间。具体调整方法本文不做描述，请参考其他文档。