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:<u>http://1</u>92.168.0.109/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。

ficrosoft 证书服务 peap	
下载 CA 证书、证书链或 CRL	
要信任从这个证书颁发机构颁发的证书, <u>安装此 CA 证书链</u> 。	
要下载一个 CA 证书、证书链或 CRL,选择证书和编码方法。	
CA 证书:	
编码方法:	
ODER Opase 64	
下载 CA 证书 下载 CA 证书链 下载最新的基 CRL	

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

Kicrosoft 证书服务 CAMS-CA
欢迎
使用此网站为您的 Web 浏览器,电子邮件客户端或其他程序申请一个证书。通过使用证书,您可以向通过 Wi 署并加密邮件,并且,根据您申请的证书的类型,执行其他安全任务。
您也可以使用此网站下载证书颁发机构(CA)证书,证书链,或证书吊销列表(CRL),或查看挂起的申请的状态
有关证书服务的详细信息,请参阅 <u>证书服务文档</u> .
<u> 选择一个任务: 車遺一个证书</u> 查看挂起的证书申请的状态 下载一个 CA 证书,证书链或 CRL
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】:
ficrosoft 证书服务 CAMS-CA
申请一个证书
选择一个证书类型: <u>Web 浏览器证书</u> <u>电子邮件保护证书</u>
或者,促父一们 <mark>、<u>局级证书中</u>谊。</mark>
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】:
ficrosoft 证书服务 CANS-CA
高级证书申请
CA 的激略决定您可以申请的证书类别。单击下列选项之一来: <u>创建并间此 CA 提文一个申请。</u> 使用 base64 编码的 CMC 或 PMCS #10 文件提文 一个证书申请, 或使用 base64 编码的 PMCS #7 文件续订证书申请。
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】:
Iicrosoft 证书服务 peap
高级证书申请
识别信息:
9至名: heserver 电子邮件: he@h3c.com
소리: h3c
市/县: [bj
省: bj
需要的证书类型:
服务群身份验证证书 💌
密钥选项: ④创建新宏祖集 〇 使用现存的宏祖集
CSP: Microsoft Enhanced Cryptographic Provider v1.0
密钥用法: ○交換 ○签署 ④ 問者 密钥大小: 1024
④ 自动密钥容器名称 ○ 用户指定的密钥容器名称
☑ 标记密朝为可与出 □ 导出密朝到文件
□扁用編私朝保护 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】
潜在的脚本冲突
此网站正在代表您请求一个新的证书。您应该只允许信任的网站为您请求证书。您想现在请求证书吗?
是① 【 古
图3.a 下帮服冬哭自从坠证证书于音图a





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】:

证书导出向导	×
导出文件格式 可以用不同的文件格式导出证书。	
选择要使用的格式	
◯ DER 编码二进制 X 509 (CER) ℚ)	
○ Base64 编码 X.509 (.CER) (≦)	
○加密消息语法标准 - PKCS #7 证书(PTB) ℃)	
●私人信息交換 - PKCS #12 (.PFX)(P)	
🧾 如果可能,将所有证书包括到证书路径中 🖤	
☑ 启用加强保护(要求 IE 5.0, NT 4.0 SP4 或更高版本)(图)	
🔲 如果导出成功,删除密钥 🕼	
	_
〈上一步 ④)下一步 ④)〉 取消	

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。

T 书导出向导	Σ
密码 要保证安全,您必须用密码保护私银].
键入并确认密码。	
密码 (P):	
↓ 确认密码(C):	
	〈上一步 ④)下一步 ④ 〉 取消

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】。

证书导出向导				
	正在完成证书导出向导 您已成功地完成证书导出向导。 您已指定下列设置:			
	文件名 E: \heserver.pfx 导出密钥 是 包括证书路径中所有证书 否 文件格式 个人信息交换 (*.pfx)			
34	< 上一步 (B) 完成 取消			

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

	名称 -	大小	类型	修改日期
文件和文件夹任务	3110		文件夹	2006-8-4 17:23
0.000	99		文件夹	2006-6-22 21:41
109年一1新文叶天	Program Files		文件夹	2006-8-14 14:56
将这个文件关发带到	temp		文件夹	2006-8-1 15:51
11月11日日11日	🛅 test		文件夹	2006-8-16 10:13
DW DW	i i i i i i i i i i i i i i i i i i i		文件夹	2006-8-9 18:04
	○出差报告		文件夹	2006-6-9 12:45
宅位置	会		文件夹	2006-8-16 10:16
	○ 工作周振		文件夹	2006-8-9 11:00
我的电脑			文件夹	2006-6-23 16:34
) 我的文档	一 新加速		文件夹	2006-7-24 12:35
共享文档	英语学习		文件夹	2006-6-22 20:30
9 回上報應	11111111111111111111111111111111111111		文件夹	2006-8-16 9:59
	○ 特正论文汇总		文件夹	2006-5-13 11:10
	Asserver	3 13	Personal Inform	2006-8-16 10:15

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:

Ticrosoft 证书服务	peap			
高级证书申请				_
识别信息:				
姓名: heclient				
电子邮件: he@h3c.co	om			
公司: h3c				
部门: ts				
市/县: bi				
省: bj				
国家(地区): CN				
需要的证书类型:				
客户端身份	计验证证书 🔽			
密钥选项:				
③ 创建新石	密钥集 〇使月	用现存的密钥集		
CSP: Microsoft I	Enhanced Cryptog	raphic Provider v1.0	~	
密钥用法: 〇交换	 ○签署 ○] 	两者		
密钥大小: 1024	最小值: 384 (一般语 最大值:16384	例大小: 512 1024 2048 4096 8192 16384)		
 自动密報 	月容器名称 🤇)用户指定的密钥容器名称		
☑标记室報	用为可导出			
· 두 ·	密钥到文件			
图10 生成的客户端验证	正证书示音图			
当证书安装完成后,	在控制台可	以看到该证书。如图1	1所示。	
■ 控制台1 - 【控制台根节点\证	书 - 当前用户\个人	\证书]		
白文件(2)操作(4) 查看(2) 收	· ▲ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	1b (t)		
	1.054944	10000 25		INTER OF
□ 正的日間 2月	heclient	pesp	2007-8-16	客户编验证
日 二 个人	122 heserver	24sb	2007-8-16	服务器验证
• 〇 受信任的根证书颁发机构 > 〇 全当信任				
• • 中级证书硬发机构				
 Active Directory 用户对象 受信任的发行者 	65			
····································				
● ● 受信任人				
1 🔄 证书注册申请				
图11 导出生成的客户	□端验证证‡	完成后示意图		
而而早长忠	⊨.			
凹、配直天键的	<i></i>			
1) 左昭冬哭洪		书旦田本体发安白进证	书的相证书	而左安白於

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。