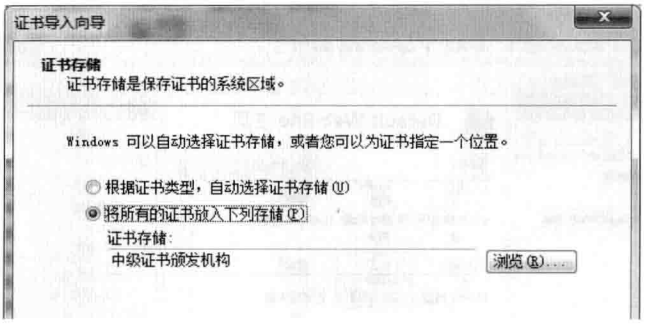

图 22-21　导入证书到“中级证书颁发机构”

⑱ 依次单击“下一步”按钮，直到完成，如图 22-22 所示。

图 22-22　导入 CA 证书到中级证书颁发机构

⑲ 至此完成证书安装。

22.1.2　配置 SSL 策略

① 在完成服务器端证书配置后，需要配置 SSL 使用策略。打开“Internet 信息服务(IIS)管理器”，在“Default Web Site”中选择“SSL 设置”，如图 22-23 所示。

② 双击“SSL 设置”，出现如图 22-24 所示的界面。勾选“要求 SSL”，在“客户证书”中有 3 个选项，分别是“忽略”、“接受”、“必需”：

- 忽略：是默认选项。不要求客户端提供有效证书，即使提供客户端证书，也会忽略掉。该选项不会要求客户端在获得内容访问权限之前验证其身份。因此，该设置在这些设置中的安全性最低。

图 22-23　SSL 配置选择

图 22-24　SSL 设置选项

- 接受：如果要接受客户端证书（若提供），并在允许客户端获得内容访问权限之前验证客户端身份，则选择该设置。
- 必需：要求客户端必须提供有效证书。选择该选项以在允许客户端获得内容访问权限之前要求证书验证客户端身份。

22.1.3　访问 Web Server

以上依次配置完成后，就可以访问支持 SSL 的 Web 了。重新启动 IIS 服务，在浏览器中输入访问地址 http://localhost，则显示图 22-25 所示的 IIS7 欢迎界面，表示配置 SSL 成功。

图 22-25　使用 https 访问 IIS 服务器

22.2　Apache 服务器证书配置

22.2.1　下载并安装服务器证书

在 Windows 环境下 Apache 的安装文件包括 32 位、64 位版本，以及 2.2.x 和 2.4.x 系列，可以从 http://www.apachelounge.com/download/下载。下面以 2.4.x 为例说明服务器证书的配置，2.2.x 的服务器证书配置也类似。假定 Apache 的安装路径为 c:/Apache2。

除了 Windows 版本，Apache 使用最多的是在 Linux 环境。在 Linux 环境下的服务器证书配置与 Windows 下基本相同。

Apache 配置文件中使用的是文件证书和私钥，其 SSL 功能由 mod_ssl 模块提供，mod_ssl 模块利用 OpenSSL 实现了 SSL 功能。如果要使用密码设备提供的私钥和密码操作，需要配置专用密码设备的信息，因密码设备不同，其配置信息也会不同，本节不讨论专用密码设备配置信息，只说明使用文件方式配置 Apache 服务器证书。

Apache 安装完成后，形成如图 22-26 所示的目录结构。

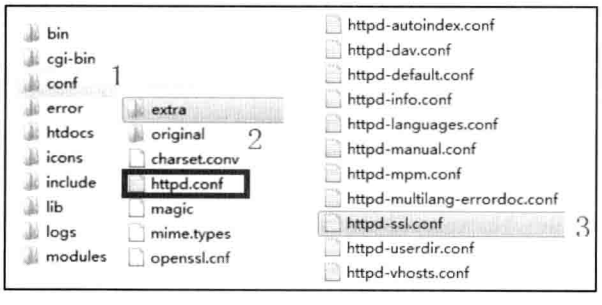

图 22-26　Windows 下 Apache 安装后的目录

在 Apache 服务器中有一个总配置文件，即 httpd.conf，位于 Apache 安装目录下的 conf 子目录中，它配置了 Apache 的主要参数。为了便于管理，SSL 的配置单独放到了 extra 子目录下的 httpd-ssl.conf 中，要启用 SSL，需要在 httpd.conf 中找到如下行：

```
#LoadModule ssl_module modules/mod_ssl.so
#LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
```

去掉 LocadModule 前面的“#”，在配置文件中以#开始的行表示是注释行，得到如下内容：

```
LoadModule ssl_module modules/mod_ssl.so
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
```

同时找到下面两行：

```
# Secure （SSL/TLS） connections
#Include conf/extra/httpd-ssl.conf
```

然后去掉 Include 前面的注释符“#”，得到如下内容：

```
# Secure （SSL/TLS） connections
Include conf/extra/httpd-ssl.conf
```

“Include conf/extra/httpd-ssl.conf”的意思是 httpd-ssl.conf 也会成为总配置文件的一部分，此处使用了文件相对路径，如果在前面加上 Apache 的安装路径就是文件的全路径（在 Apache 配置文件中使用斜线（/）分隔文件路径，而不是使用反斜线（\））。然后打开 httpd-ssl.conf 文件，查看需要配置的内容。我们只关注证书相关内容，其他配置使用默认值（如使用 443 为 HTTPS 访问端口等）。

在 httpd-ssl.conf 中找到如下信息：

```
#  Server Certificate:
#  Point SSLCertificateFile at a PEM encoded certificate.  If
#  the certificate is encrypted,  then you will be prompted for a
#  pass phrase.  Note that a kill -HUP will prompt again.  Keep
#  in mind that if you have both an RSA and a DSA certificate you
#  can configure both in parallel （to also allow the use of DSA
#  ciphers,  etc.）
SSLCertificateFile  " c:/Apache2/conf/server.crt "
```

此处要求配置服务器证书，证书格式为 PEM。继续往下找私钥配置信息：

```
#  Server Private Key:
#  If the key is not combined with the certificate,  use this
#  directive to point at the key file.  Keep in mind that if
#  you′ ve both a RSA and a DSA private key you can configure
#  both in parallel （to also allow the use of DSA ciphers,  etc.）
SSLCertificateKeyFile  " c:/Apache2/conf/server.key "
```

此处要求配置服务器的私钥，私钥可以用口令进行保护。

除了配置服务器证书和私钥外，还需要配置 CA 证书，找到如下信息：

```
#   Certificate Authority （CA）:
#   Set the CA certificate verification path where to find CA
#   certificates for client authentication or alternatively one
#   huge file containing all of them （file must be PEM encoded）
#   Note: Inside SSLCACertificatePath you need hash symlinks
#            to point to the certificate files. Use the provided
#            Makefile to update the hash symlinks after changes.
SSLCACertificateFile  " c:/Apache2/conf/ca.crt "
```

CA 证书同样以 PEM 格式表示，文件中可以包含多个 CA 证书，对于有多级证书的情况比较有用。

在使用 HTTPS 访问 Web 服务器时，要求 Web 网站的域名或 IP 地址必须是服务器证书的通用名（commonName）。下面还是使用 OpenSSL CA 产生 Apache 服务器证书私钥，并配置完成 CA 证书。

1．产生证书请求

执行命令产生证书请求：

```
openssl.exe req -newkey rsa:1024 -days 360 -keyout .\demoCA\private\server.key -keyform PEM -out .\demoCA\server.req -outform PEM -nodes -subj " /C=CN/CN=localhost "
```

为了演示方便，产生的服务器私钥文件没有加密（在正式生产环境中，需要使用保护口令对私钥文件进行加密），私钥文件的内容为：

```
-----BEGIN PRIVATE KEY-----
MIICdQIBADANBgkqhkiG9w0BAQEFAASCAl8wggJbAgEAAoGBAKwY2ZD5dsOIAaa+
PxOYUrUPOT3JI5Gk3JzbH/0LuyH69VjsTd5moV+zyWg9qsllqa6IqwHLwP//ikly
WBNQ9BDz8tTH2Yq53m0C73ePF5NgQOExpTFZ8CPINQBjcojqOOn/DCnTwpVnC/E4
8psLTWTA0IJ0tt2WGaGUCYgn6GD7AgMBAAECgYBIune3fLVkDKYmAWBGt6i8O6LF
KauOcU2KPFBYcAy1X4kv+y0tP9ISz7feBbGXSw9aYwdhyunVRfj68Qenoh6CGckc
FE41EEDlRR/LBJo6knhsiqt99pVZSiWM/Fb6lsvbg/ceTwW4XPu9YKcRgrO6y2m/
1FrnhR6XhIZcWzSqgQJBAOBUfvdvee36v0Ix1OZneA5I3TZGx1a2KalL1ke15gLC
ycwT4XXdd0TZcveujOY0xWOZZJev8MTBkdPY9sy+F58CQQDEZJp1qWymtqsu34BO
uLEqKIh2yKsQzUctRFj48hvmXdmoE1Nm4Q5unoGKug12iTDlrVNq51B/D1R9zlwZ
yaklAkBEAPlYUv/YZ6nxDCApFHatheMhYAVvwNsSSj4UEQ1ACwKXjfNMAq30PiL+
+HgYFSk9TzPSU/CeBLwLR3tRh9KrAkA9+imsfB0nt3nqPuo07aArV8NJCSbDFKUj
qfASEAWx+2gW3JJzYw605hyndPOOttjRgpNSp1EF6AaX9SmnkbZpAkB245moB9tc
EjDybU1gwX1PvnUKVnfVo8wtJT05eoHqH/bI+1e04sQUSjWxrydPNLNvG0lawIYD
ZewJg+jS0mfJ
-----END PRIVATE KEY-----
```

2．签发证书

执行命令签发证书：

```
openssl.exe ca -in .\demoCA\server.req -out server.crt -days 360
```

签发后的证书如图 22-27 所示。