证书管理器（CertMgr）2.x
用户安装使用手册

2002-10

上海市电子商务安全证书管理中心有限公司

Shanghai Electronic Certificate Authority center co.,ltd

文档说明：

本文档介绍了证书管理器（CertMgr**）**ver2.20 **及其以上版本的安装及使用操作过程的说明。**

版本信息：

2.21 CertMgr 2002-10-16

版权信息：

SHECA 是上海市电子商务安全证书管理中心有限公司的注册商标和缩写。

本文的版权属于上海市电子商务安全证书管理中心有限公司，未经许可，任何个人和团体不得转载、粘贴或发布本文，也不得部分的转载、粘贴或发布本文，更不得更改本文的部分词汇进行转贴。

未经许可不得拷贝，影印。

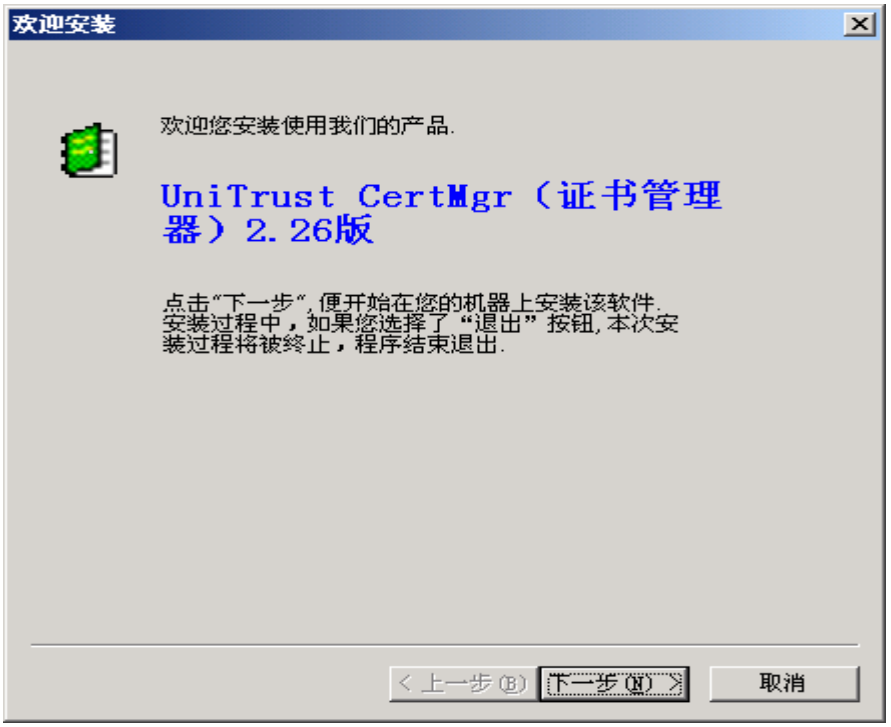
Copyright @2000 上海市电子商务安全证书管理中心有限公司

证书管理器安装

证书管理器的安装程序提供了标准的 Windows 向导式的安装方式，用户依照安装提示便可顺利的进行证书管理器的安装，将证书管理器安装到本地机器中，以便操作使用。

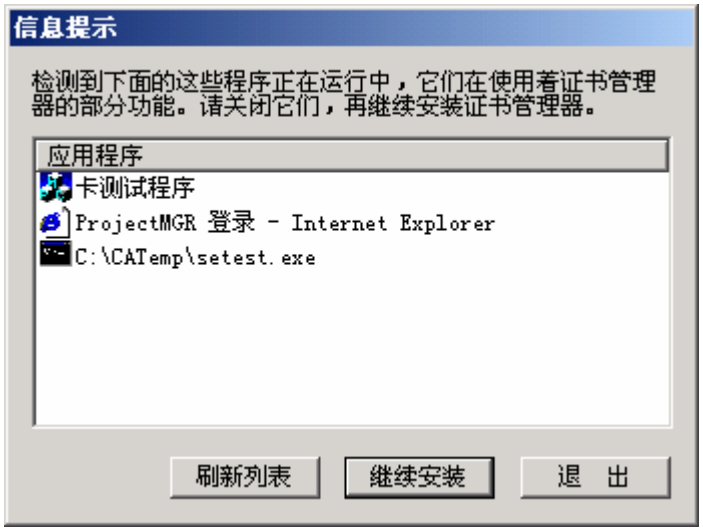
安装步骤：

1、在 SHECA 提供的安装光盘中（或从 SHECA 网站上 http://www.sheca.com/service/download.htm 下载获得)找到证书管理器的安装目录，找到并双击提供的证书管理器的安装文件 “ setup.exe ”，执行安装。

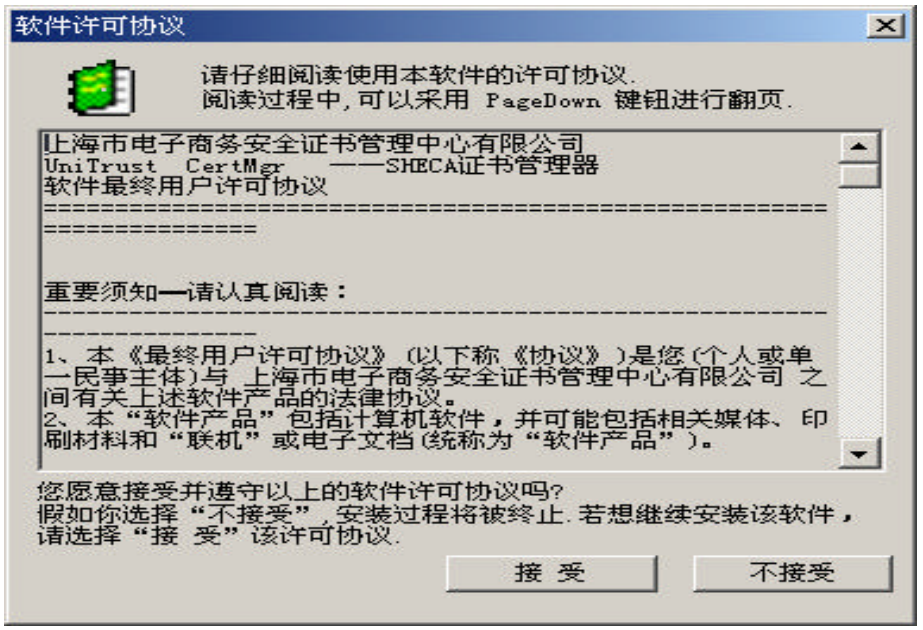


在 WindowNT/2K/XP 环境下，点击下一步，则弹出安装环境的检测条,开始对证书管理器的安装环境进行检测。若安装环境检测通过，则继续下一步的安装，否则提示相应的检测出错信息，指导用户进行相应的操作。

如：安装时,检测到当前有些运行的程序正在使用证书管理器的部分功能时，则会列出所有的那些程序的名字，要求用户先关闭掉那些程序，再进行下一步的安装。

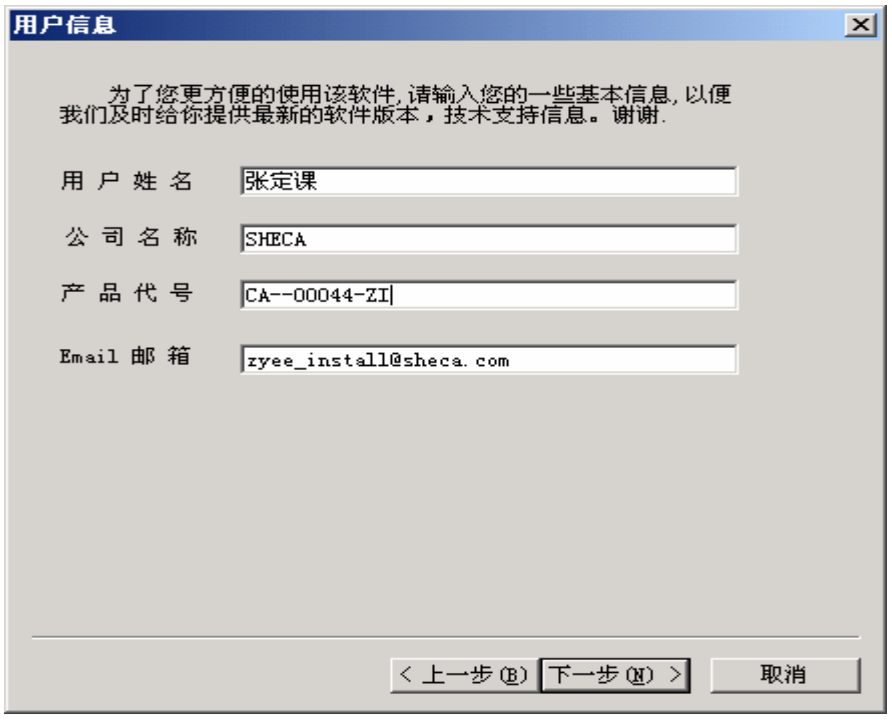


2、 **接受软件许可协议。**

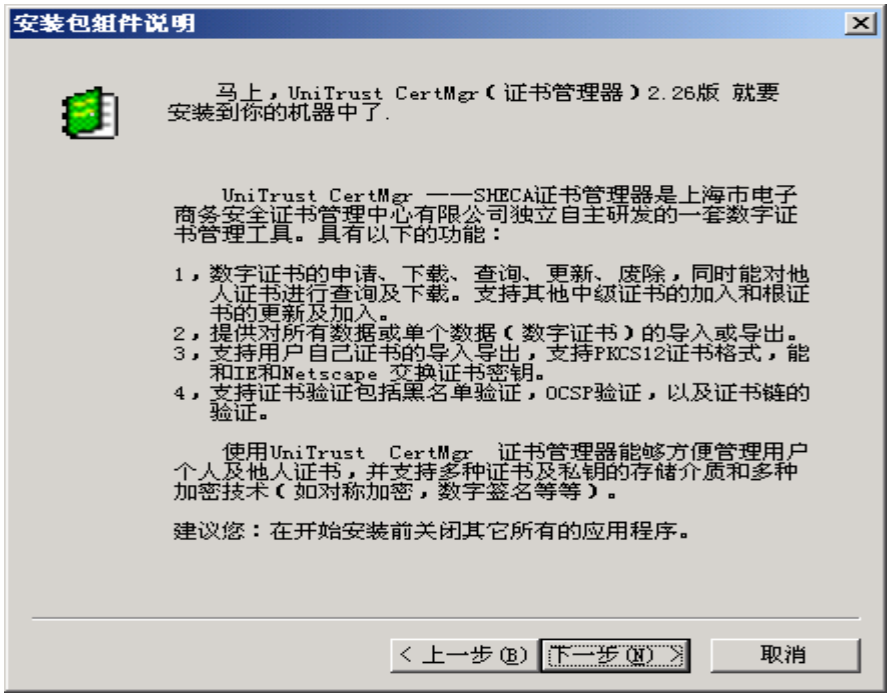


假如用户选择“ 不接受 ”软件允可协议，安装过程将被终止，请 选择“ 接 受 ”软件允可协议，继续安装证书管理器。

3、**注册正确的用户信息。**

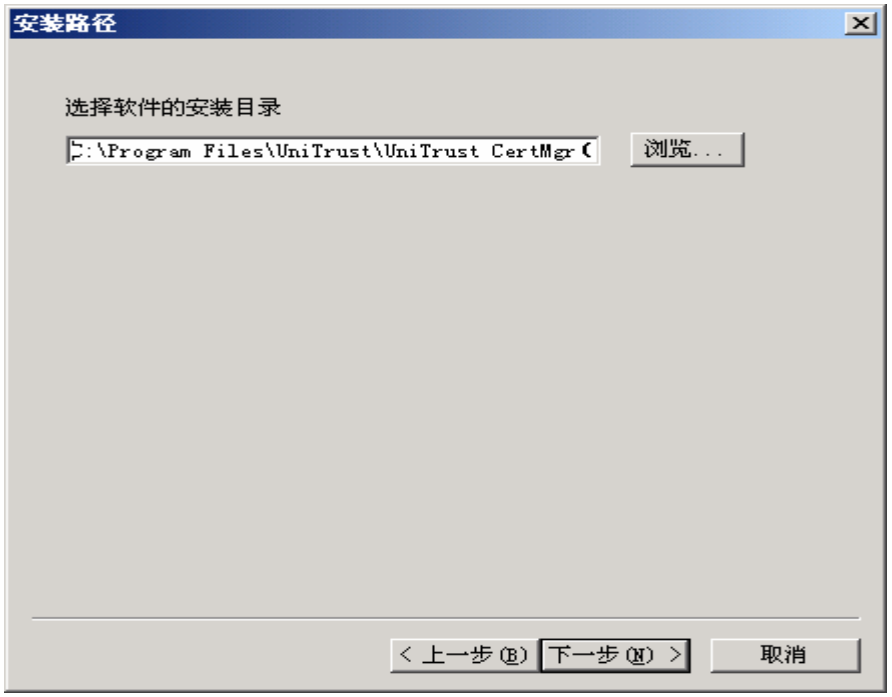


4、查看安装包组件说明。

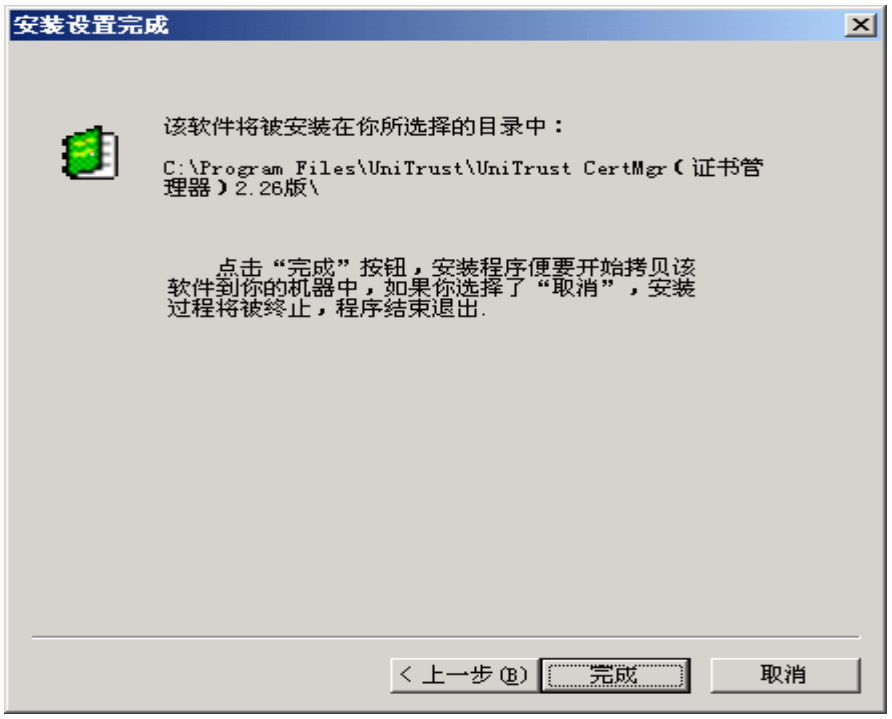


5、用户可通过“浏览”来选择证书管理器安装路径，程序默认的安装路径是：

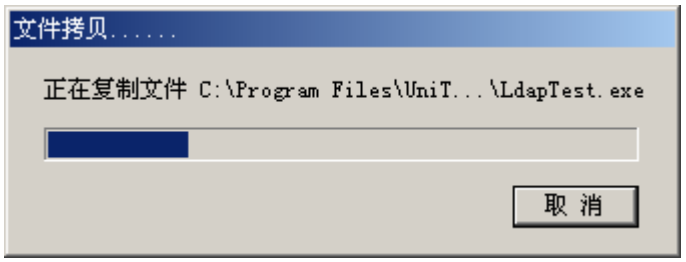
%Root%:\%program Files%\UniTrust\UniTrust CertMgr（证书管理器）。



6、**完成证书管理器的安装设置。**



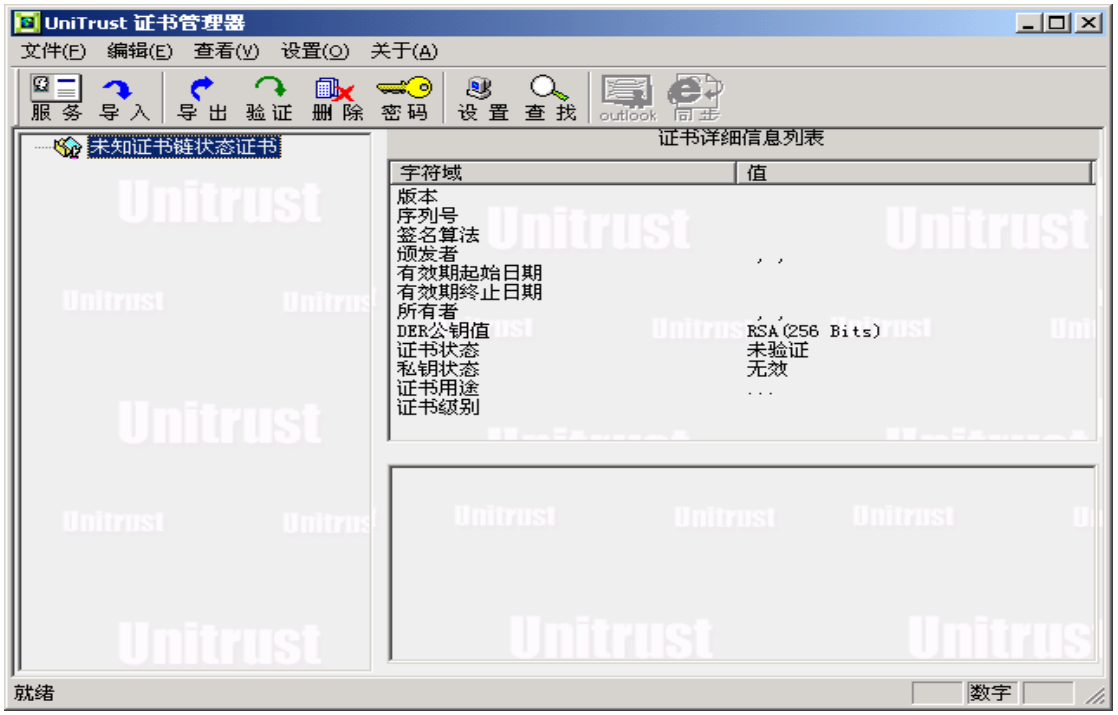
7、**安装程序将文件复制到用户指定的安装目录。**



8、证书管理器安装成功。

9、重新启动机器，然后通过系统 开始菜单 → 程序 → SHECA 证书管理器，运行刚刚安装过的 SHECA 证书管理器，以确认安装过程顺利完成。

SHECA 证书管理器安装后第一次运行主界面截图如下



卸载证书管理器

SHECA 证书管理器成功安装后，会在系统菜单“ 开始->程序 ”中生成新的菜单项“ SHECA 证书管理器 ”，点击其中的的“ Inst_Z 卸载安装 ”，便弹出证书管理器的卸载确认框，用户选择“ 确定 ”，则开始卸载本地机器上安装过的 SHECA 证书管理器。

用户亦可通过选择系统“ 控制面板 ”中的“ 添加/删除功能项 ”，来删除安装过的 SHECA 证书管理器。

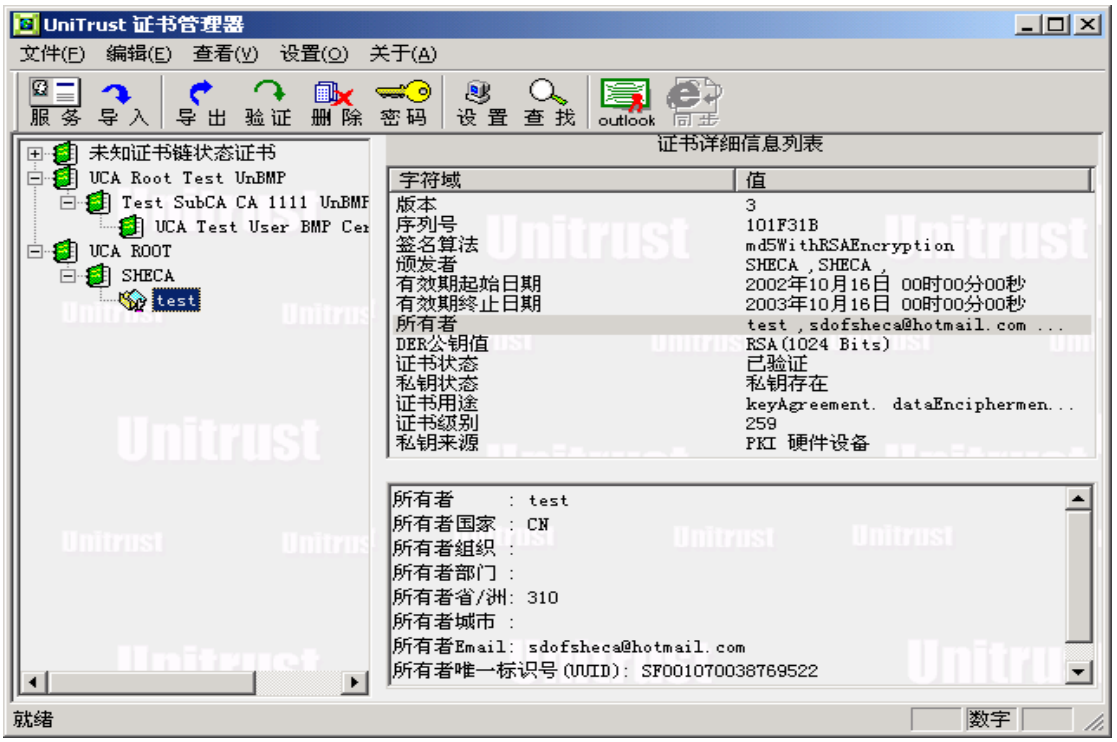
注意在卸载证书管理器前，请导出证书管理器里相关的用户证书，以作备用。

证书管理器使用

证书管理器简介

UniTrust 证书管理器 是 SHECA **针对广大数字证书用户推出的一个简单易用的客户端软件，用户通过它可以方便地维护，管理和使用自己及他人的数字证书,如 私钥密码修改，证书更新，发送安全邮件 等。**

UniTrust **证书管理器主操作界面采用** Windows **系统文件浏览器方式列出用户当前所有的证书。**



其中，左侧的列表框内显示的是当前用户所有的证书以及相应的证书链信息,选中每条证书，则在右边的列表框内显示出该张证书的主要信息，如 证书持有人姓名(DN)，邮件地址,唯一标识号，证书签发者信息，证书的状态信息，证书级别,证书用途等等。 用户若进一步选中列表框条目，下面的信息框将显示更为详细的信息。

利用证书管理器提供的菜单，工具条，用户可以简单，快捷进行证书别名更改，证书(或 PKCS12 **格式)导出，导入，查找证书，证书服务等一系列常规的证书管理工作。**

下面按照用户常规的证书操作功能，逐一详细地讲述证书管理器的使用方法。

？． 证书服务 

SHECA **网站上具有很多的针对数字证书功能性服务,如 证书策略公布，**SHECA **公告，**CRL **证书状态查询等等，用户若需要相关的**SHECA **在线证书服务功能，可以点击主操作**

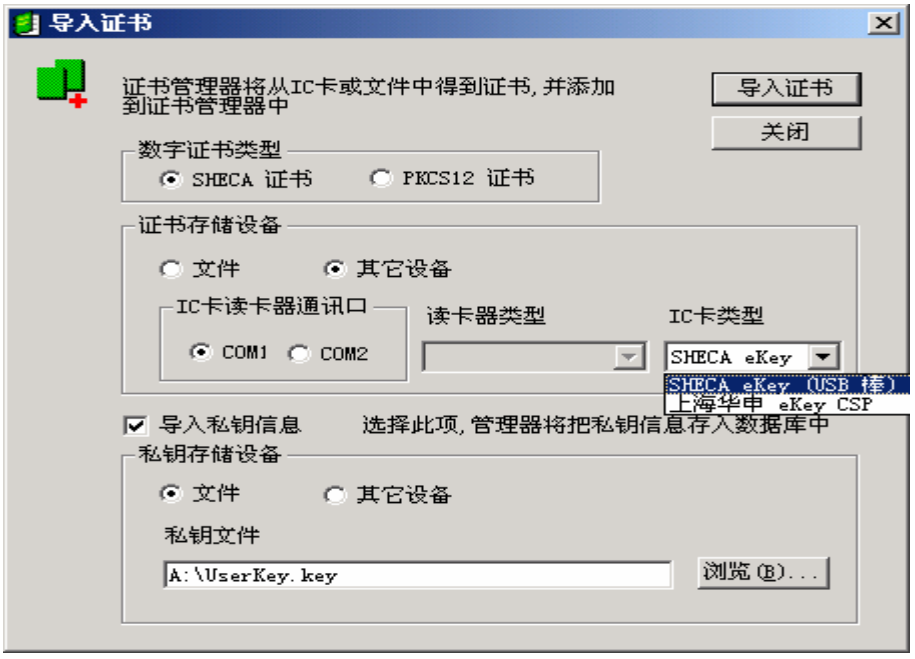
界面菜单项中的“文件→证书服务”或工具栏上的“ 服务 ”图标，便能进入到SHECA 相应的数字证书服务页面，浏览，查找自己所需的在线服务功能项。

二. 导入证书 导入

添加外部证书(或含私钥信息)到证书管理器中。

一般的，用户从SHECA 申请获得了数字证书时，证书一般存储在文件，PKI 设备，或PKCS12 格式中。其中，文件格式是SHECA 根据用户需求制定的一种格式，即命名文件UserCert.der 为用户证书， UserKey.key为用户私钥文件，一同递交给用户。PKI 设备指用户通过SHECA 认证的一些 PKI设备来申请、存储证书和私钥文件。PKCS12 格式是国际上一种通用的数字证书和私钥信息一起封装打包的格式，由众多的网络浏览器所支持，如Microsoft IE，Netscape。证书管理器导入外部证书时，支持 文件，PKI 设备，PKCS12 这三种格式。

注意：导入外部文件形式证书的过程中，证书管理器会读取与证书相同路径下的一个名为 CertChain.spc 的文件，该文件为SHECA 颁发给用户的证书信任链文件。若该文件不存在，证书管理器会自动从一些自带的默认证书信任链文件来查找匹配，若还是找不到,则将该证书添加到“未知证书链状态”。



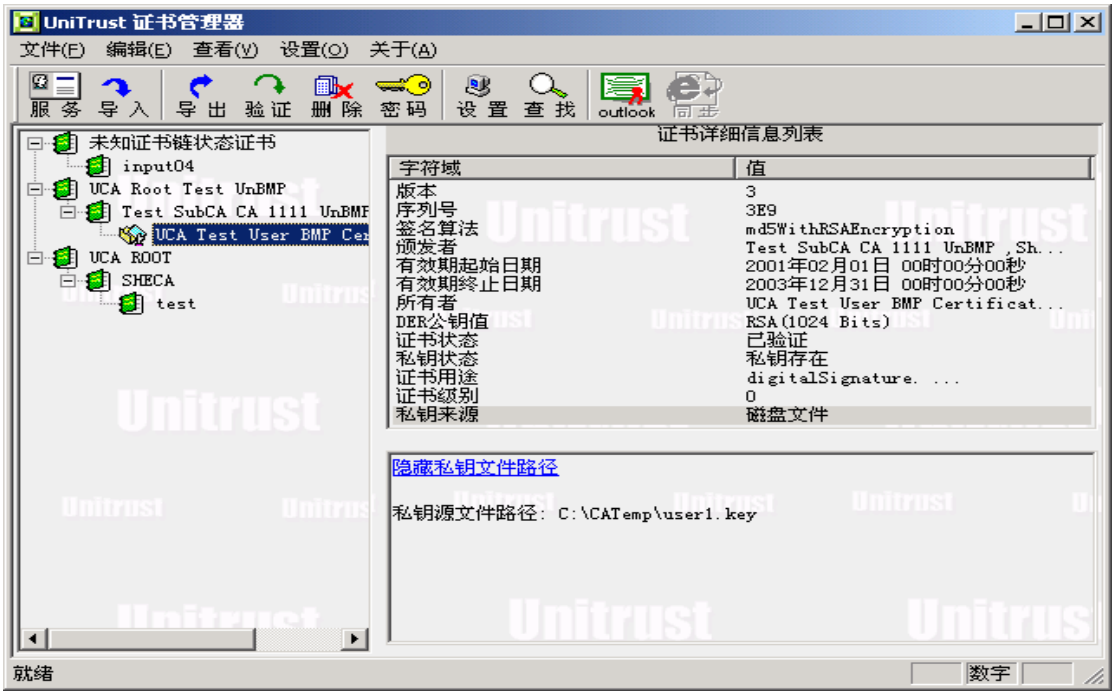
点击主操作界面菜单项中的“文件→导入证书”或工具栏上的“ 导入 ”图标，便打开了“导入证书”对话框。

文件证书导入：

1. “数字证书类型”选择“SHECA证书”,“证书存储设备“ 和“私钥存储设备”选择 “文件”。（默认选择 ）
2. 点击“浏览。。。”按钮，选择证书和私钥文件的具体路径。默认为读取软盘中（A:）的用户证书文件 UserCert.der 和私钥文件 UserKey.key。
   若仅导入证书文件，则将复选框“导入私钥信息”置为未选中 状态。(该复选框默认为选中状态)
3. 点击“导入证书”按钮，证书管理器便将证书添加到证书管理器中。若选择要导入私钥信息，则会弹出一个私钥保护密码的输入校验框，用户输入正确的私钥保护密码后，证书管理器便将证书和私钥信息一同添加进去。

若证书连同私钥信息一同导入，则在证书管理器主界面“证书详细信息栏”的“私钥状态”项中，显示为“私钥存在”，否则，显示为“私钥不存在”。
若导入了私钥信息,则在“私钥来源”项中，会显示私钥的相关存储信息。

(小技巧： 证书管理器支持对文件证书的 “拖动” 导入，即在系统的文件浏览器中选中后缀名为 der 或 key 的文件，拖动到证书管理器的窗口中，便会自动的添加到证书管理器中，方便快捷)

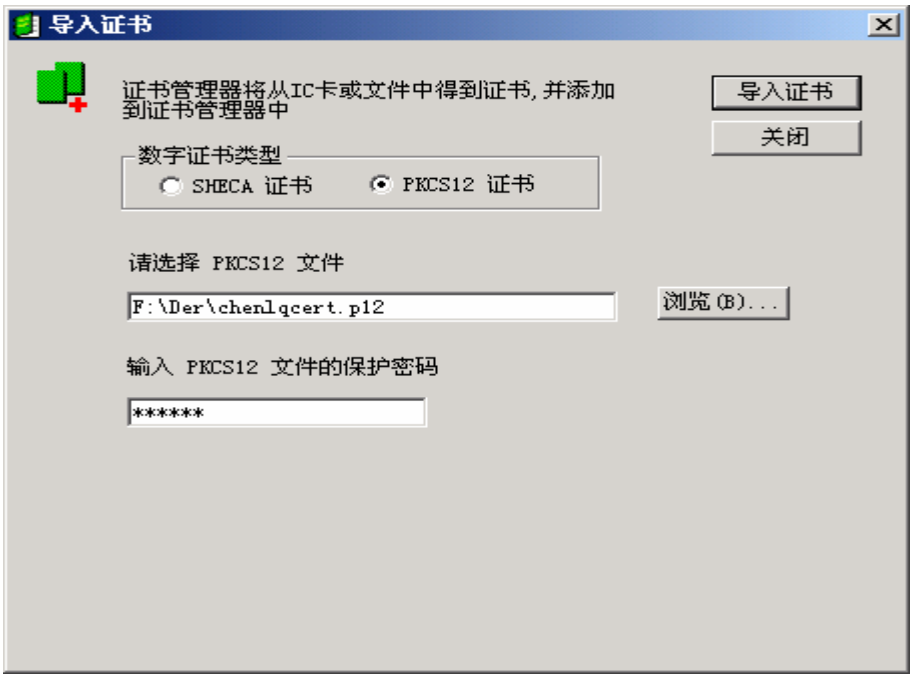


PKI 证书导入：

操作步骤同上，在数字证书类型栏中选中“其它设备”，然后选择正确的“IC 卡类型”和“读卡器类型”便可。

PKCS12 证书导入：

“数字证书类型”选择“PKCS12 证书”，点击“浏览。。。”按钮选择PKCS12 证书的具体路径，输入PKCS12 文件的保护密码便可。



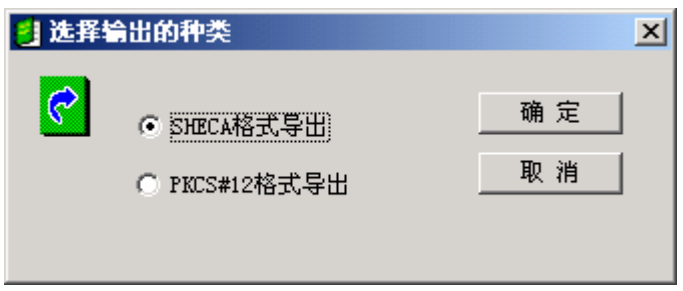
三. 导出证书 

从证书管理器中以文件形式导出用户证书(或含私钥信息)到磁盘上。

证书管理器支持两种导出格式：SHECA 文件格式和通用PKCS12 格式。其中 SHECA 文件格式是以磁盘文件形式导出用户证书(或私钥)到磁盘上。PKCS12 格式导出仅限于那些含有私钥信息的用户证书。

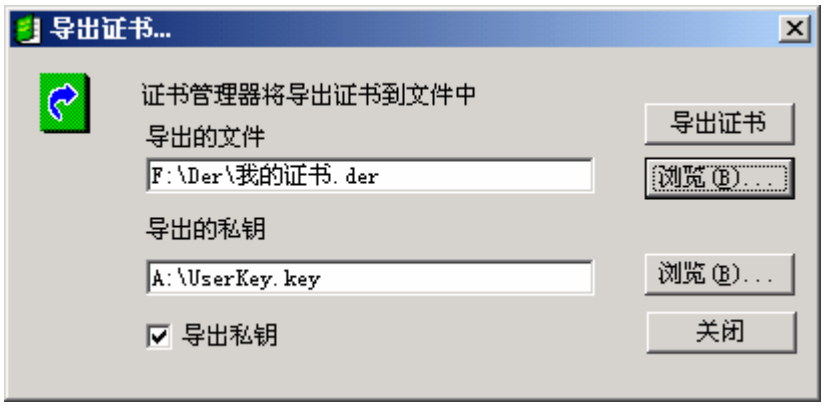
点击主操作界面菜单项中的“文件→导出证书”或工具栏上的“ 

” 图标，便可开始导出当前主界面中选定的用户证书。首先打开 “选择输出的种类”对话框：



SHECA 格式导出(默认)

在导出证书的保存路径框中，用户可指定证书的具体保存路径，证书默认导出路径为A:\UserCert.der，私钥默认导出路径为 A:\UserKey.key。在导出私钥过程中，用户需正确输入私钥的保护密码，进行使用身份确认。



PKCS12 格式导出

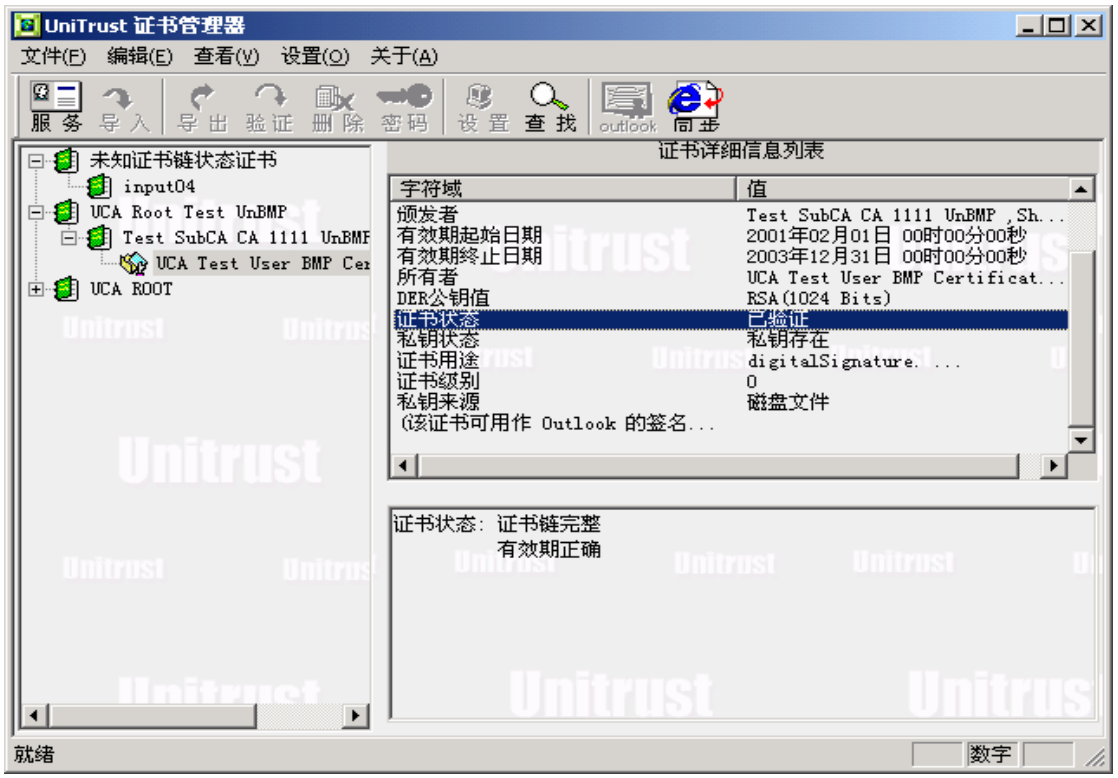
在导出证书的保存路径框中，用户可指定PKCS12 证书的具体保存路径。导出过程中，用户需输入正确的私钥保护密码，进行使用身份确认。
（注：当前证书管理器中，PKCS12 格式导出仅限于那些含有私钥信息的用户证书）

四. 校验证书状态 

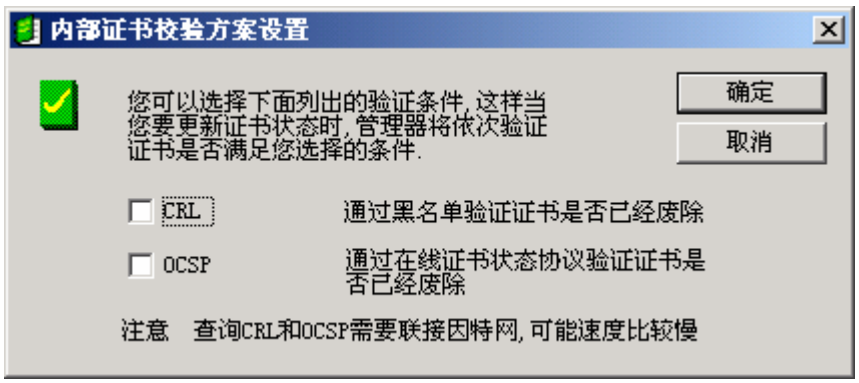
对选定证书的状态进行在线验证,显示证书的有效状态值。

一般的，在证书管理器中，用户证书的基本状态包含两个方面的校验值：证书链完整性和证书的有效期。每张用户证书在加入到证书管理器时，都会对基本证书状态进行验证，验

证后的状态值在主界面的“证书详细信息列表”中的“证书状态”栏显示出来。

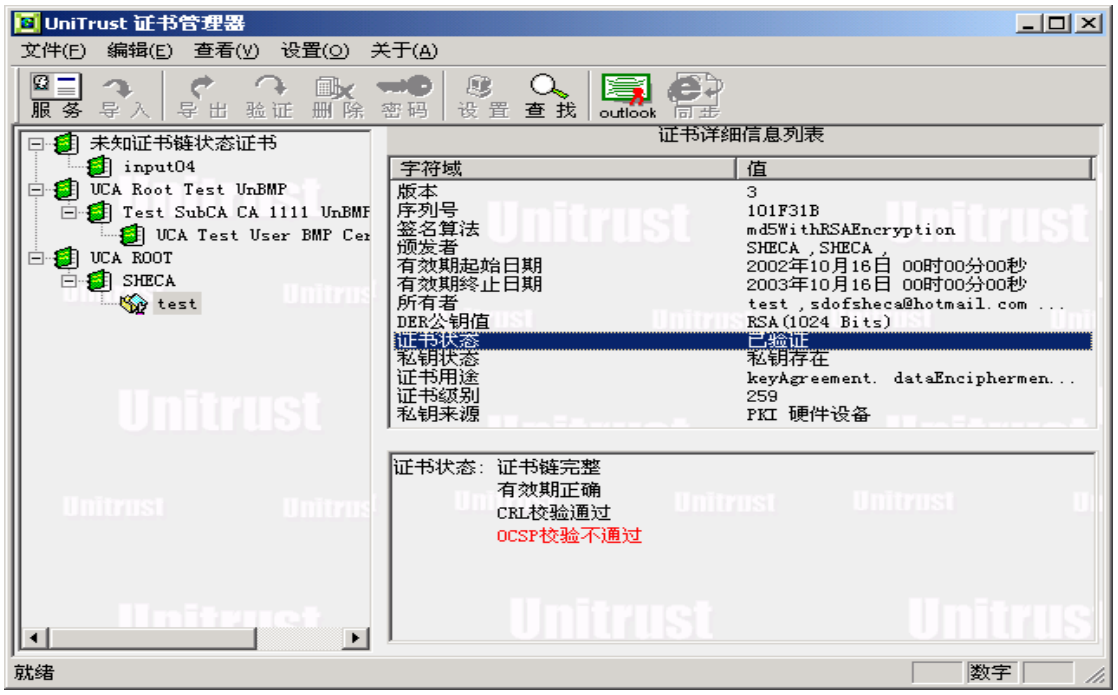


用户若想获得更多证书的状态校验值，如 CRL 验证值（证书废除黑名单），OCSP 验证值（在线证书状态验证），可以点击工具栏按钮“  ”或主菜单项“设置-→内部证书验证方案设置”，弹出“证书验证方案设置”对话框，可进行证书状态验证方案设置，设置完毕，点击“确定”按钮保存当前设置信息。



在主界面中，点击“  ”便会采用当前设置的验证方案对证书进行动态验证。验证完毕，在“证书详细信息列表”中的“证书状态”栏显示出新的证书状态值。

注意，有些验证设置方案，如 CRL、OCSP 验证，需要通过因特网连接到SHECA 的相关服务器 获取信息，可能验证操作速度较慢，请耐心等候。



五. 删除证书 

从证书管理器中删除当前选定的证书。

在弹出的证书删除确认框中，用户若选择“确定”，则会从证书管理器中彻底删除该张证书(和相应私钥信息)。若被删除的证书为根级证书，则该根级证书所签发的所有用户证书都将转到未知证书链状态下。未知证书链状态的用户证书稍后可通过“ 匹配完整证书链 ”功能重新查找到相应的证书链信息。

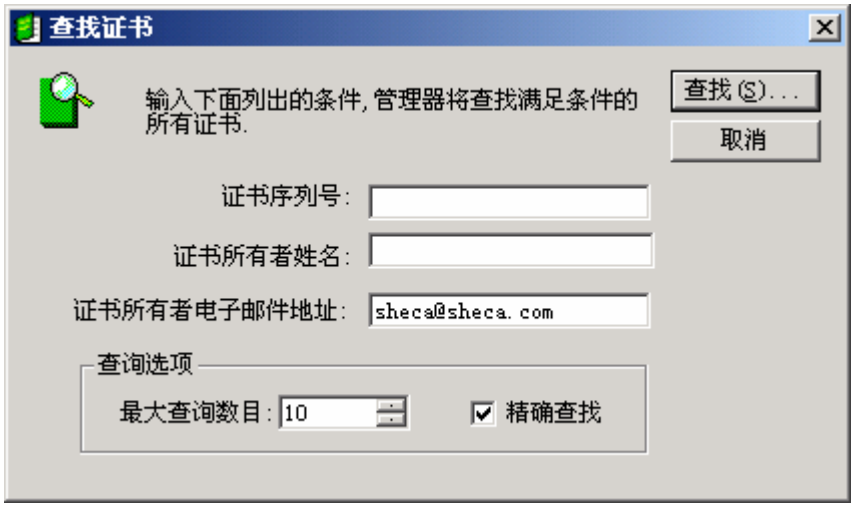
点击工具栏按钮“  ”或主菜单项“编辑->删除证书”,便可以进行证书的删除操作。证书删除支持键盘“Delete”键操作。

六. 查找证书 

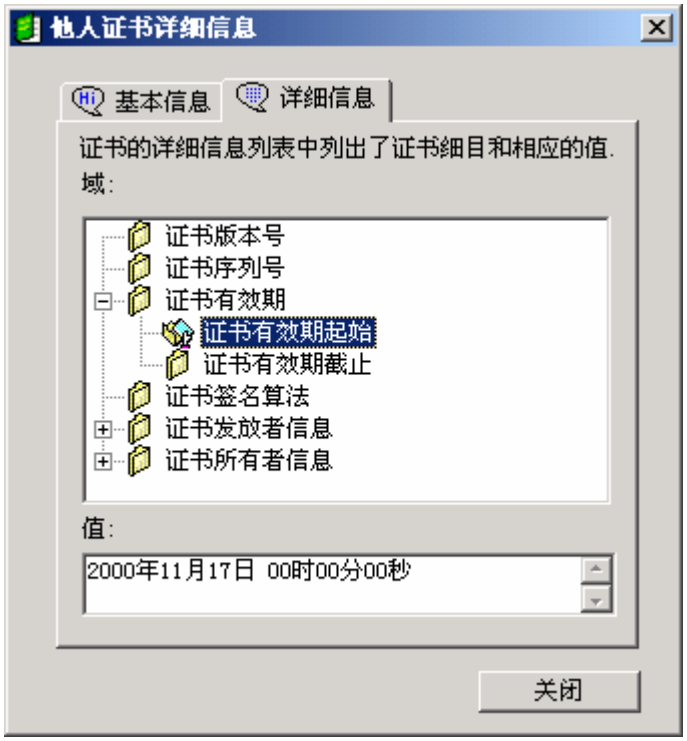
从 SHECA LDAP 证书服务器上获取其他人的证书。

对于每个签发成功的用户证书，sheca在相应的LDAP 服务器中进行发布，供用户日后进行证书查询或软件开发商开发使用。点击工具栏按钮“ 查找 ”或主菜单项“ 查看-→查找证书 ”，便可以从LDAP 服务器中查找证书。证书管理器默认的LDAP 服务器URL为ldap://ldap2.sheca.com:389，用户若需查找其他LDAP上发布的证书，可以打开菜单项“ 设置-→LDAP 服务器信息设置 ”，选择所需的LDAP 服务器地址：

开始查找证书时，用户需输入一个或多个查询过滤条件，以便快速的查找到所需的证书，如输入待查询证书的序列号，证书所有者姓名，Email 地址。还可以设定查找过程是否需要“ 精确查找 ”，若选择“ 精确查找 ”，则根据用户输入的查询过滤条件，从LDAP 服务器上查找出信息完全与之匹配的的所有证书，否则，进行“ 模糊查询 ”，查找出所有信息与查询过滤条件相近或类似的证书。用户还可以设定查询结果中返回的证书个数，仅需更改界面中编辑框“ 最大查询数目 ”的数目值便可。推荐的最大查询数目为 10。



查询出来的所有用户证书以列表框方式列出，选定一张证书，双击鼠标便可以查看到该张证书的详细信息，用户此时亦可选择将证书直接加入到证书管理器中，以便日后用。



七. 修改私钥密码 

修改与用户证书相对应的私钥保护密码。

SHECA 为签发的每张证书对应的私钥信息都进行了加密保护处理,用户在使用私钥过程中(如 数字签名),需正确输入私钥的保护密码。一般的，私钥初始保护密码为用户在SHECA受理点申请时所用到的密码信封中8 位长度的字符串。

点击工具栏按钮“ 

”或主菜单项“ 编辑-→修改私钥密码 ”,便可以修改当前主界

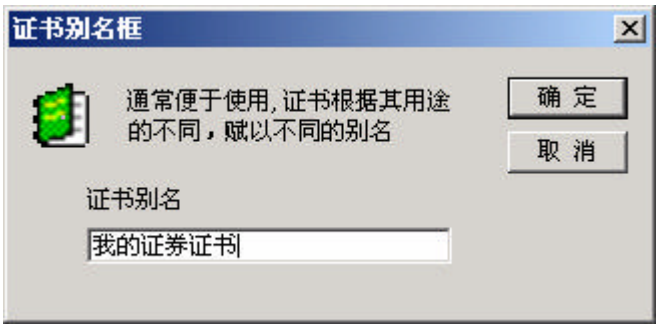
面里选中证书对应的私钥保护密码。

注意，在修改“私钥来源”为 磁盘文件的私钥文件的保护密码时，证书管理器不仅更改证书管理器里面的私钥文件保护密码，同时也会修改私钥源文件的保护密码，用以保证用户私钥保护密码的同步性。

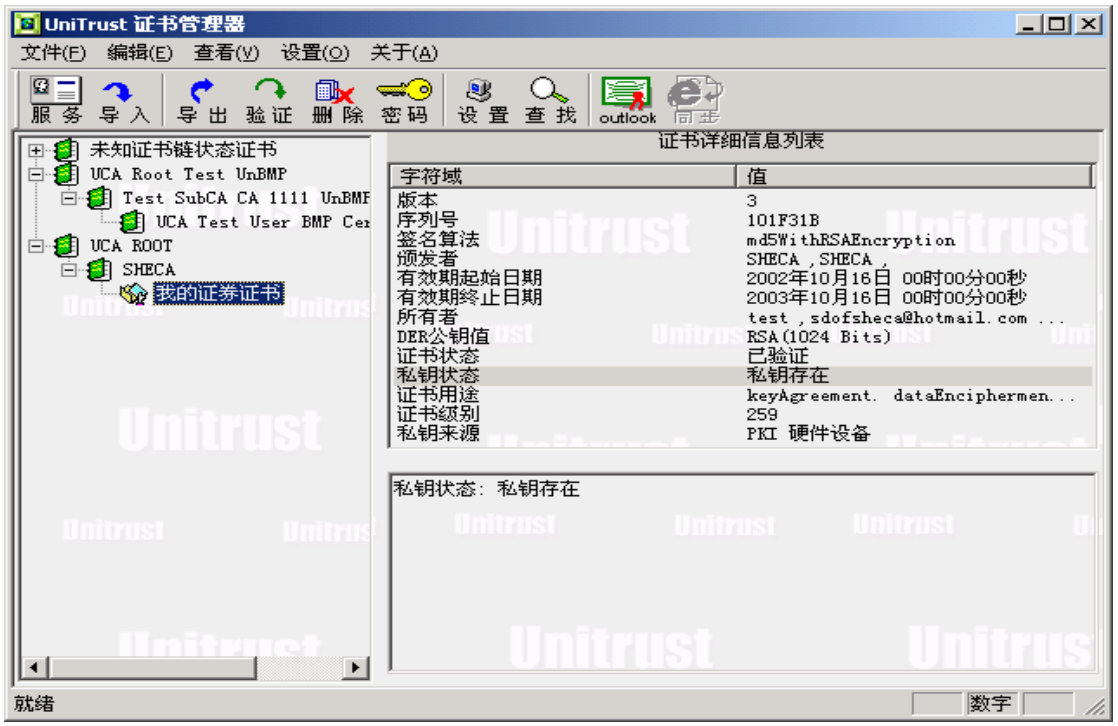
八. 更改证书别名

根据证书的用途对证书设置不同的别名。

主界面证书浏览窗口中，选中用户证书，点击鼠标右键，弹出菜单，点击“更改证书别名”，便弹出证书别名设置框，用户可为证书设置所需的别名。



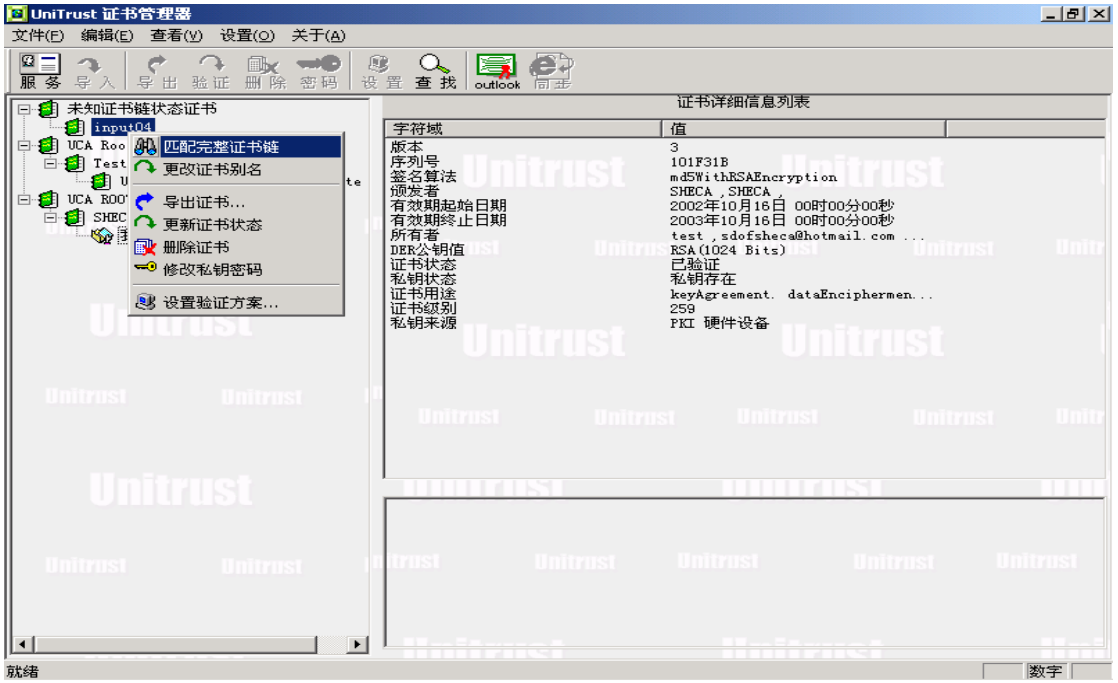
证书别名设置完毕，在主界面右侧的证书名称浏览列表中，便能看到新设置的别名名称。



九. 匹配证书链信息

重新查找，匹配证书相应的证书链信息。

主界面证书浏览窗口中，选中用户证书，点击鼠标右键，弹出菜单，选定 “匹配完整证书链 ”,便开始重新匹配与证书对应的SHECA 证书链信息，匹配成功后，则该张证书自动移动到证书链的分支下面，便于日后使用。



证书链信息管理说明：

SHECA 签发用户证书的同时，一般也会颁发给用户一个名为 Certchain.spc 的证书链文件，该证书链文件里包含有用户证书对应的所有的SHECA 根级证书，各级根证书间以链式结构延伸，采用国际通用 Pkcs8 标准进行编码，共同标识用户证书与顶级SHECA 根证书之间的唯一身份继承关系。当前SHECA 颁发的证书链中共有两级根证书，No.1 级根证书通用名称为 “UCA ROOT”，No.2 级根证书通用名称为”SHECA”，它们内置于证书管理器中，用户安装好证书管理器，便可使用该证书链信息。证书链信息常以 Certchain.spc 文件形式与用户证书一起颁发给用户，也可以保存于SHECA 认证推荐的各类 PKI 设备中，用户从SHECA 的网站上也可下载获得SHECA 相应的证书链文件。

证书管理器在管理证书链信息时，不同于一般的用户证书管理。一般的，证书链中的各级根证书不允许进行一些常规的用户证书操作，如 证书别名设置，匹配证书链等。删除根级证书时，证书管理器也只是将该根级证书签发的用户证书转移到“ 未知证书链状态 ”下，根级证书信息并未真正从证书管理器中删除掉。

用户进行“ 匹配完整证书链 ”操作时，证书管理器查找内部所有的根级证书,包括原先执行了“ 删除 ”操作的根级证书，对用户证书进行根证书校验匹配，找到匹配的根证书。若在证书管理器内部未能找到与用户证书相匹配的根级证书，则证书管理连接因特网，到 SHECA 相应的LDAP 服务器上查找相应的证书链信息，找到后下载新的证书链信息到本地，否则将该张用户证书转移到“ 未知证书链状态 ”下，证书基本状态验证值设为不通过。

十. 添加为 Outlook 安全邮件签名证书

添加用户证书（含有私钥信息）到 Windows 系统证书库中，作为 Outlook 安全邮件的签名加密证书，供其它基于 Windows CryptoAPI 开发的应用系统利用。这样用户的证书就能够广泛的应用于各个领域，如 SSL 安全通道，软件发布商代码签名等等。

该功能仅限于SHECA 证书管理器 ver2.25 及以上版本。

要想获得更多有关这方面的帮助信息，请参阅文档 “UniTrust CSP 用户安装使用手册”。

十一. 网上升级

为了获得 SHECA 公司发布的最新证书管理器版本或升级信息，请访问上海市电子商务安全证书管理中心有限公司网站 http://www.sheca.com/service/download.htm.，在那里您可以下载到最新版本的 SHECA 证书管理器，获得更多的相关信息和帮助信息。