Red Hat Certificate System 10

使用企业安全客户端管理智能卡

为 Red Hat Certificate System 10.1 更新

Last Updated: 2023-05-10

Red Hat Certificate System 10 使用企业安全客户端管理智能卡

为 Red Hat Certificate System 10.1 更新

Florian Delehaye
Red Hat Customer Content Services
fdelehay@redhat.com

Marc Muehlfeld
Red Hat Customer Content Services

Petr Bokoč
Red Hat Customer Content Services

Marc Muehlfeld
Red Hat Customer Content Services

Filip Hanzelka
Red Hat Customer Content Services

Ella Deon Ballard
Red Hat Customer Content Services

Tomáš Čapek
Red Hat Customer Content Services

法律通告

摘要

本指南适用于证书系统子系统的常规用户。它解释了如何使用企业安全客户端管理个人证书和密钥，这是一个简单的接口来格式化和管理智能卡。

目录

第 1 章 企业安全客户端简介

企业安全 *客户端是* Red Hat Certificate System 的一个工具，简化了管理智能卡。最终用户可以使用安全令牌(smart 卡)来存储应用程序的用户证书，如单点登录(SSO)访问和客户端身份验证。最终用户签发令牌，其中包含签名、加密和其他加密功能所需的证书和密钥。

企业安全客户端是证书系统的完整令牌管理系统的第三部分。两个子系统 - 令牌密钥服务(TKS)和令牌处理系统(TPS)- 用于处理与令牌相关的操作。企业安全客户端是允许智能卡和用户访问令牌管理系统的接口。

注册令牌后，可将 Mozilla Firefox 和 Thunderbird 等应用程序配置为识别令牌并将其用于安全操作，如客户端身份验证和 S/MIME 邮件。企业安全客户端提供以下功能：

- 支持与全局平台兼容智能卡，如 Gemalto 64K V2 和 Safenet 300J Java 智能卡。
- 注册安全令牌，以便 TPS 识别它们。
- 维护安全令牌，如使用 TPS 重新注册令牌。
- 提供有关被管理令牌或令牌的当前状态的信息。
- 支持通过 TPS 和 DRM 子系统生成服务器端密钥，以便在令牌丢失时，可以在单独的令牌上存档并恢复密钥。

1.1. RED HAT ENTERPRISE LINUX、单点登录和身份验证

网络用户通常必须为他们使用的不同服务提交多个密码，如电子邮件、Web 浏览和服务器，以及网络上的服务器。维护多个密码并持续被提示输入它们，对于用户和管理员而言是个。*单点登录* 是一种配置，管理员可以创建单个密码存储，以便用户可以使用单一密码登录一次，并对所有网络资源进行身份验证。

Red Hat Enterprise Linux 支持多个资源的单点登录，包括登录工作站和解锁屏保器、使用 Mozilla Firefox 访问加密的网页，并使用 Mozilla Thunderbird 发送加密电子邮件。

单点登录对用户以及服务器和网络的其他安全层都方便。单点登录在安全有效验证方面隐藏，企业安全客户端会合并到红帽认证系统实施的公钥基础架构中。

建立安全网络环境的下角之一是确保访问权限仅限于有权访问网络的人员。如果允许访问，用户可以 *向系统进行身份验证*，这意味着他们可以验证其身份。一种这样的方法是显示 *证书* ：一个电子文档，用于标识出示的实体。

这些证书可以存储在智能卡中。当用户插入时，智能卡向系统显示证书并标识用户，以便对其进行身份验证。Red Hat Enterprise Linux 单点登录的两个验证方法之一是智能卡验证。（另一个是基于 Kerberos 的身份验证。）

使用智能卡进行单点登录通过三个步骤：

1. 用户在卡读取器中插入智能卡。这由 Red Hat Enterprise Linux 上的可插拔验证模块(PAM)检测到。
2. 系统将证书映射到用户条目，然后将智能卡上出示的证书与用户条目中存储的证书进行比较。
3. 如果针对密钥分发中心(KDC)成功验证了证书，则允许用户登录。

企业安全客户端管理智能卡，这是管理单点登录的一部分。

1.2. RED HAT CERTIFICATE SYSTEM 和 ENTERPRISE SECURITY CLIENT

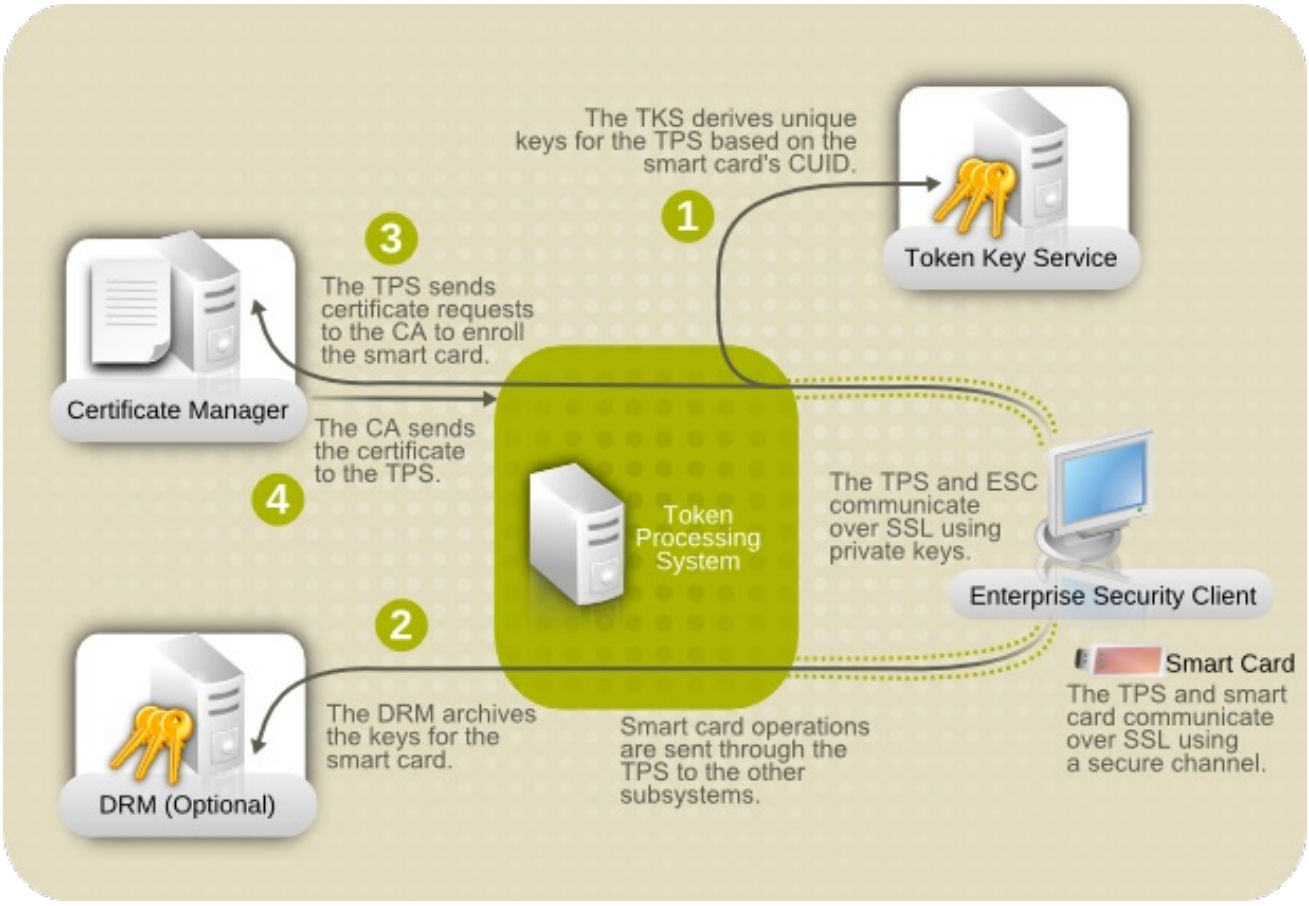
Red Hat Certificate System 创建、管理、续订和撤销证书和密钥。要管理智能卡，证书系统有一个令牌管理系统来生成密钥、创建证书请求和接收证书。

两个子系统 - 令牌密钥服务(TKS)和令牌处理系统(TPS)- 用于处理与令牌相关的操作。企业安全客户端是允许智能卡和用户访问令牌管理系统的接口。

管理令牌涉及四个证书系统子系统，两个用于管理令牌(TKS 和 TPS)，两个用于管理公钥基础架构(CA 和 DRM)中的密钥和证书。

- 令牌处理系统(TPS)与智能卡交互，以帮助它们为特定实体（如用户或设备）生成和存储密钥和证书。智能卡操作通过 TPS 进行，并转发到适当的子系统以进行操作，如生成证书或数据恢复管理器以归档和恢复密钥的证书颁发机构。
- 令牌密钥服务(TKS)生成或派生用于 TPS 和智能卡之间的通信的对称密钥。TKS 生成的每组键都是唯一的，因为它们基于卡的唯一 ID。密钥在智能卡上格式化，用于加密智能卡和 TPS 之间的通信或提供身份验证。
- 证书颁发机构(CA)会创建并撤销保存在智能卡中的用户证书。
- （可选）数据恢复管理器(DRM)存档并恢复智能卡的密钥。

图 1.1. 证书系统如何管理智能卡



如 图 1.1 “证书系统如何管理智能卡” 显示，TPS 是 Red Hat Certificate System 令牌管理系统中的中央中心。令牌直接与 TPS 通信。然后，TPS 与 TKS 通信，以生成一组可用于 TPS-token 通信(1)的唯一密钥。注册智能卡时，会为令牌创建新的私钥；如果配置了密钥归档，这些密钥可以在 DRM (2)中存档。然后，CA 处理证书请求(3)并发布要存储在令牌上的证书。TPS 将这些证书发回到企业安全客户端(4)），并将其保存到令牌。

企业安全客户端是 TPS 通过安全 HTTP 通道(HTTPS)与证书系统通信各个令牌的共识。

要使用令牌，令牌处理系统必须能够识别并与它们通信。首先必须 *注册* 令牌，以使用所需的密钥和证书填充令牌，并将令牌添加到证书系统中。企业安全客户端为最终用户提供注册令牌的最终实体的用户界面。

第 2 章 安装企业安全客户端

2.1. 客户端支持的平台

Enterprise Security Client 接口在 Red Hat Enterprise Linux 7.3 及更新的版本上被支持。

ESC 也支持最新版本的 Red Hat Enterprise Linux 5 和 6。虽然这些平台不支持 Red Hat Certificate System 10，但这些客户端可用于 Red Hat Certificate System 10 中的 TMS 系统。

2.2. 支持的智能卡

详情请查看 Red Hat Certificate System 10 发行注记 中的对应部分。

2.3. 在 RED HAT ENTERPRISE LINUX 上安装和卸载企业安全客户端

2.3.1. 安装 ESC 客户端

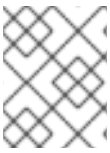
安装企业安全客户端的第一个步骤是下载所需的软件包。获取软件包的方法有两种：

- 从客户门户网站下载 ISO 镜像。
- 使用 Red Hat **yum** 工具

获取 RPM 的首选方法是使用 **yum** 命令行工具，如下所示：

```
# yum install esc
```

如果 **yum** 命令成功完成，则所有必需的企业安全客户端 RPM 和依赖项都将安装并可供使用。



注意

如果您使用 **yum** 工具安装企业安全客户端，则不需要进一步安装；客户端已经安装。以下流程是从 CD 镜像安装的步骤。

1. 以 **root** 用户身份，安装 Enterprise Security Client 软件包：

```
# yum install esc
```

企业安全客户端位于 Red Hat Enterprise Linux 32 位系统的 **/usr/lib/esc-1.1.0** 中，以及 Red Hat Enterprise Linux 64 位系统上的 **/usr/lib64/esc-1.1.0**。**esc** shell 脚本安装在 **/usr/bin/esc** 中。您可以通过运行 **esc** 命令启动企业安全客户端。

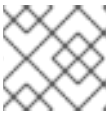
Linux 的企业安全客户端实施一个静默运行的守护进程(**escd**)，等待插入智能卡。插入未注册的智能卡时，守护进程会自动启动客户端 UI，企业安全客户端则指导用户完成注册过程。也可以通过选择 **System Settings**，然后从 **System** 菜单手动启动客户端，然后选择 **智能卡管理器**。

2.3.2. 卸载 ESC 客户端

1. 拔出所有 USB 令牌。
2. 停止企业安全客户端。

3. 以 **root** 用户身份登录，并使用 **rpm -ev** 删除企业安全客户端 RPM：

```
# yum remove esc
```



注意

更新 RPM 文件的版本号以匹配您的版本。

4. 删除安装目录中任何剩余的文件。

第 3 章 使用企业安全客户端

以下小节包含有关将企业安全客户端用于令牌注册、格式化和密码重置操作的基本说明。

3.1. 企业安全客户端的栏图标

许多程序在栏或通知区域中维护一个图标，可用于控制程序的操作，通常是在右键单击图标时通过上下文菜单。企业安全客户端提供遍历图标，包括对错误和操作的工具提示，如插入或删除智能卡。

图 3.1. Token Tray Icon 和 Tooltip 示例

在默认配置中，企业安全客户端启动并自动最小化到栏。在 Red Hat Enterprise Linux 上，只有在启用了 Gnome 中的通知区域时，才会出现栏图标。

3.2. 启动企业安全客户端

启动企业安全客户端有两个概念。必须启动企业安全客户端进程，并静默运行，等待任何插入的智能卡或令牌。当插入智能卡或手动打开时，企业安全客户端的用户界面会自动打开。

3.2.1. 在 Red Hat Enterprise Linux 上打开企业安全客户端

从命令行启动企业安全客户端守护进程(**escd**)：

```
esc
```

这个守护进程侦听智能卡，并在插入智能卡后立即打开 GUI。

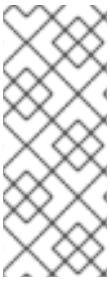
要手动打开企业安全客户端 GUI，请单击 **Applications**、**System Settings**，然后点 **Smart Card Manager**。

3.3. 配置附件主页

企业安全客户端中的 *Phone Home* 功能将每个智能卡中的信息与指向不同 TPS 服务器和企业安全客户端 UI 页面的信息相关联。每当企业安全客户端访问新的智能卡时，它可以连接到 TPS 实例并检索 phone Home 信息。

手机主页检索并缓存此信息；因为信息在本地缓存，因此每次插入格式化的智能卡时，就不必联系 TPS 子系统。

每个密钥或令牌的信息可能会有所不同，这意味着可以为不同的公司或客户组配置不同的 TPS 服务器和注册 URL。通过电话主页，可以为不同的签发者或公司单元配置不同的 TPS 服务器，而无需手动配置企业安全客户端来查找正确的服务器和 URL。



注意

要让 TPS 子系统利用 Phone Home 功能，必须在 TPS 配置文件中启用 Phone Home，如下所示：

```
op.format.userKey.issuerinfo.enable=true
op.format.userKey.issuerinfo.value=http://server.example.com
```

3.3.1. 关于附件主页配置文件

企业安全客户端基于 Gnome。当企业安全客户端缓存每个令牌的信息时，这些信息会存储在用户的配置文件中。下次启动企业安全客户端时，它会从配置文件检索信息，而不是再次联系服务器。

插入智能卡并触发了 phone Home 时，企业安全客户端首先检查 *Phone Home URL* 的令牌，这是企业安全客户端用来尝试连接到 TPS 的默认 URL。

如果没有对令牌相关的信息，用户可以通过单击企业安全客户端 UI 中的 Phone Home 按钮来手动指定

Phone Home URL 值。请参阅 第 3.3.2 节 "设置 phone Home URL"。当令牌格式化时，会提供并存储其他信息。在这种情况下，公司为用户提供了特定的 Phone Home URL。用户提交 URL 后，格式过程会将其余信息添加到 Phone Home 配置集。用户的格式进程没有任何不同。

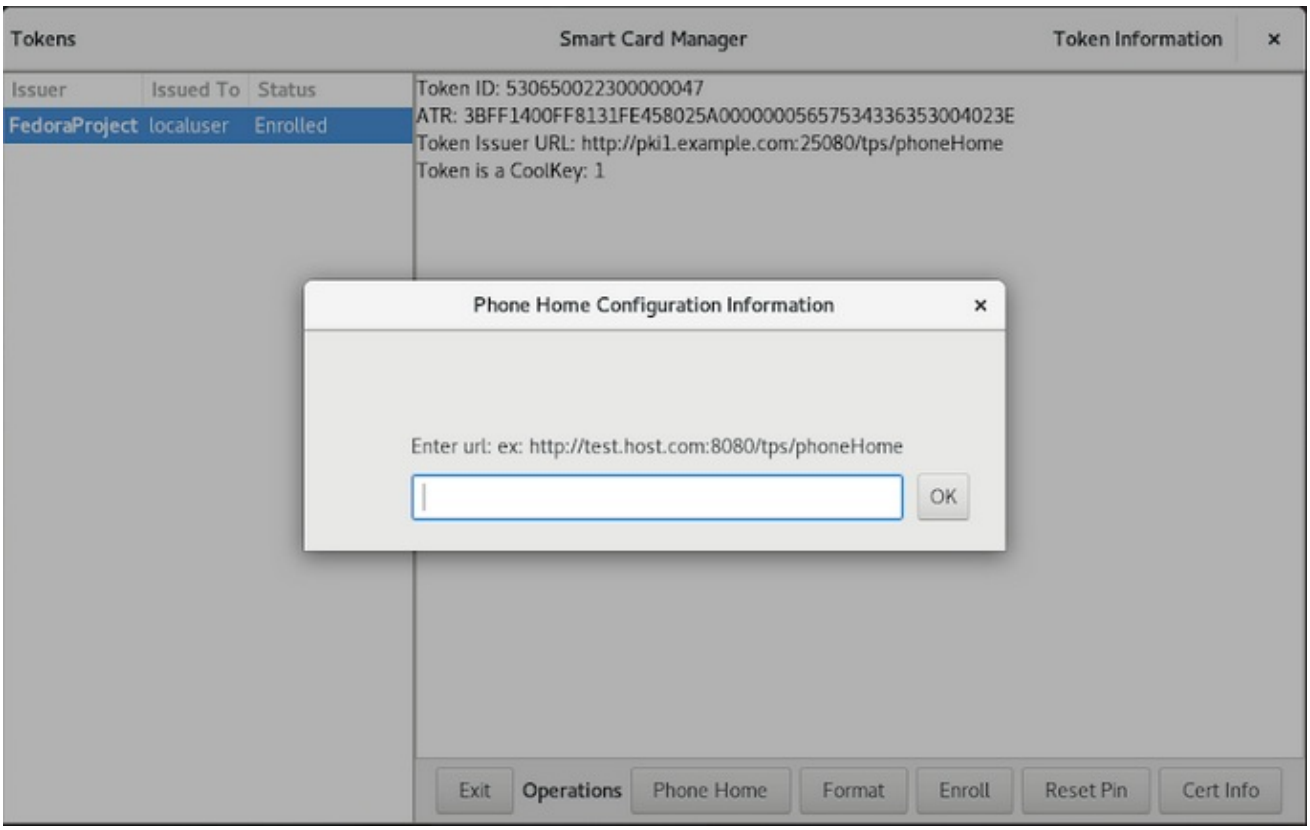
3.3.2. 设置 phone Home URL

企业安全客户端需要配置为与 TPS 通信；这通过 phone *Home URL* 来完成。格式化令牌（它们可由制造商或您的 IT 部门进行格式化）已设置此 URL。如果令牌未格式化，企业安全客户端无法找到 phone Home URL：此类空白令牌需要手动定义 URL。

Phone Home 按钮允许用户指定 Phone Home URL：

1. 插入空白令牌后，单击企业安全客户端 UI 中的 **Phone Home** 按钮以打开配置对话框。
2. 在 **TPS Config URI** 字段中，填写新的 TPS URL。
3. 单击 **OK** 保存。正确配置了新的 Phone Home URL 后，检索其余信息并添加到 Phone Home 配置集中。

图 3.2. 电话主页 URL 配置



3.3.3. 将 TPS 配置为使用附件主页

Phone Home 功能及其使用不同类型的信息仅在正确配置 TPS 时使用 phone Home 时才起作用。如果没有，TPS 会忽略此功能。电话主页在 **/var/lib/pki/pki-tomcat/tps/conf/** 目录中的 **phoneHome.xml** 中配置；这会将 phone Home 信息输出到 XML。

例 3.1 "TPS Phone Home 配置文件" 显示 TPS 子系统用于配置 phone Home 功能的 XML 文件示例。

例 3.1. TPS Phone Home 配置文件

```
<ServiceInfo><IssuerName>Example Corp</IssuerName>
```

```
    <Services>
      <Operation>http://server.example.com:7888/nk_service ## TPS server URL
      </Operation>
      <UI>http://server.example.com:7888/cgi_bin/esc.cgi   ## Optional
Enrollment UI
      </UI>
      <EnrolledTokenBrowserURL>http://www.test.url.com   ## Optional
enrolled token url
      </EnrolledTokenBrowserURL>
    </Services>
</ServiceInfo>
```

TPS 配置 URI 是 TPS 服务器的 URL，它将其余信息返回给企业安全客户端。这个 URL 的示例是 **http://localhost:8443/tps/phoneHome**; URL 可以根据需要引用机器名称、完全限定域名或 IPv4 或 IPv6 地址。当访问 TPS 配置 URI 时，TPS 服务器会提示您将所有 phone Home 信息返回给企业安全客户端。

要测试智能卡服务器的 URL，请在 **TPS Config URI** 字段中输入地址，然后单击 **Test URL**。

如果服务器成功联系，则消息框表示成功。如果测试连接失败，则会出现错误对话框。

3.4. 将用户设置为注册

安装令牌处理系统后，其配置设置之一就是 LDAP 目录，其中包含允许注册令牌的用户。只有存储在此身份验证目录的用户才能注册、格式化或具有令牌。在尝试注册令牌或智能卡前，请确保请求操作的人员在 LDAP 目录中有一个条目。

TPS 配置为查看 LDAP 目录中的特定基本 DN。这在 TPS 的 **CS.cfg** 中配置：

```
auth.instance.0.baseDN=dc=example,dc=com
auth.instance.0.hostport=server.example.com:389
```

要使用户被允许注册令牌，用户必须是基本 DN 下的某个位置。

如果用户还没有条目，则管理员必须将用户添加到指定基本 DN 中的指定 LDAP 目录中，然后才能为用户注册任何令牌。

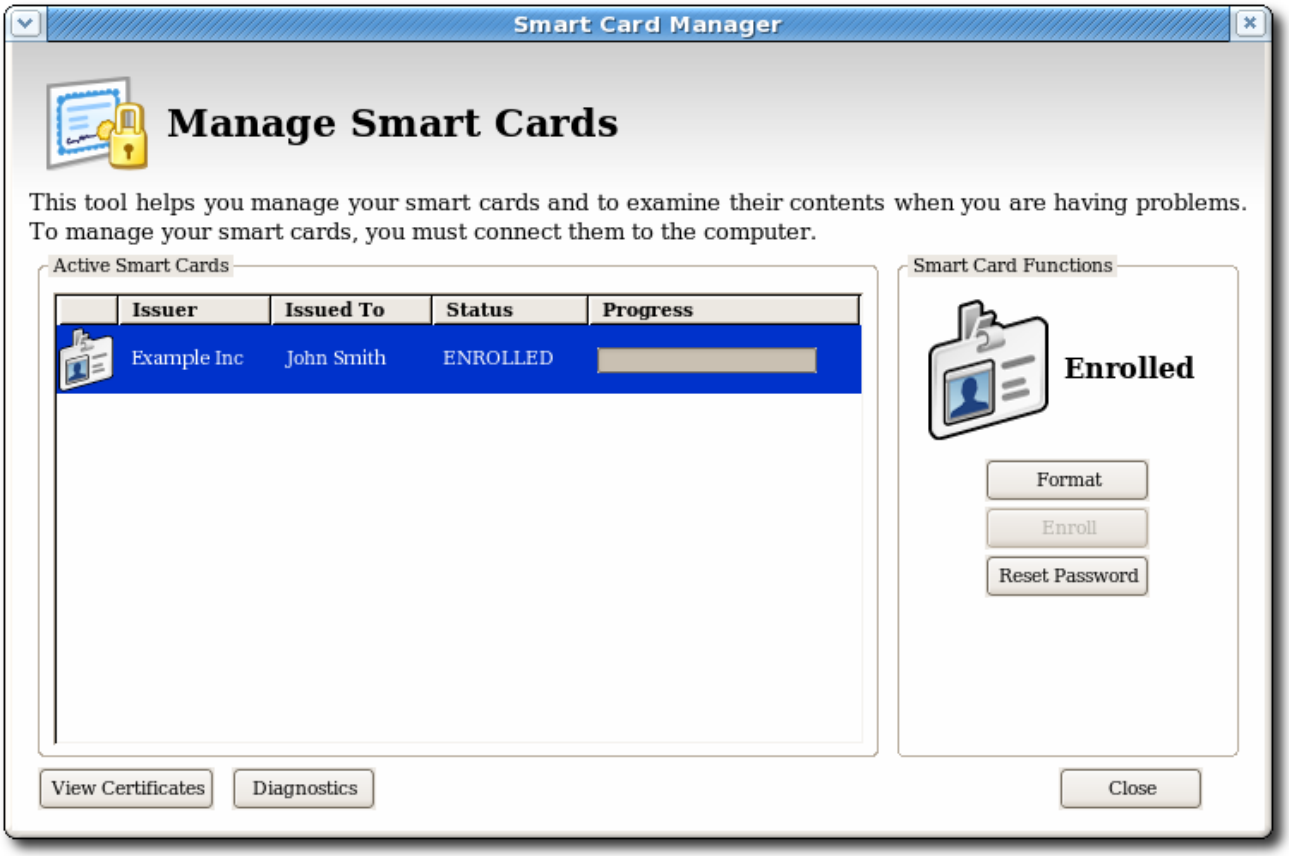
```
/usr/bin/ldapmodify -a -D "cn=Directory Manager" -w secret -p 389 -h server.example.com

dn: uid=jsmith,ou=People, dc=example,dc=com
objectclass: person
objectclass: inetorgperson
objectclass: top
uid: jsmith
cn: John Smith
email: jsmith@example.com
userPassword: secret
```

3.5. 管理智能卡

您可以使用 **Manage Smart Cards** 页面执行许多可应用到令牌中存储的加密密钥的操作。

您可以使用此页面格式化令牌，设置和重置卡的密码，并显示卡信息。另外，也可以通过 **管理智能卡** 页面访问其他两个操作，即注册令牌和查看诊断日志。这些操作在其它部分中解决。

图 3.3. 管理智能卡页面



3.5.1. 格式化智能卡

当您格式化智能卡时，它会重置为未初始化的状态。这会删除所有之前生成的用户密钥对，并在注册过程中清除智能卡上设置的密码。

格式化智能卡：

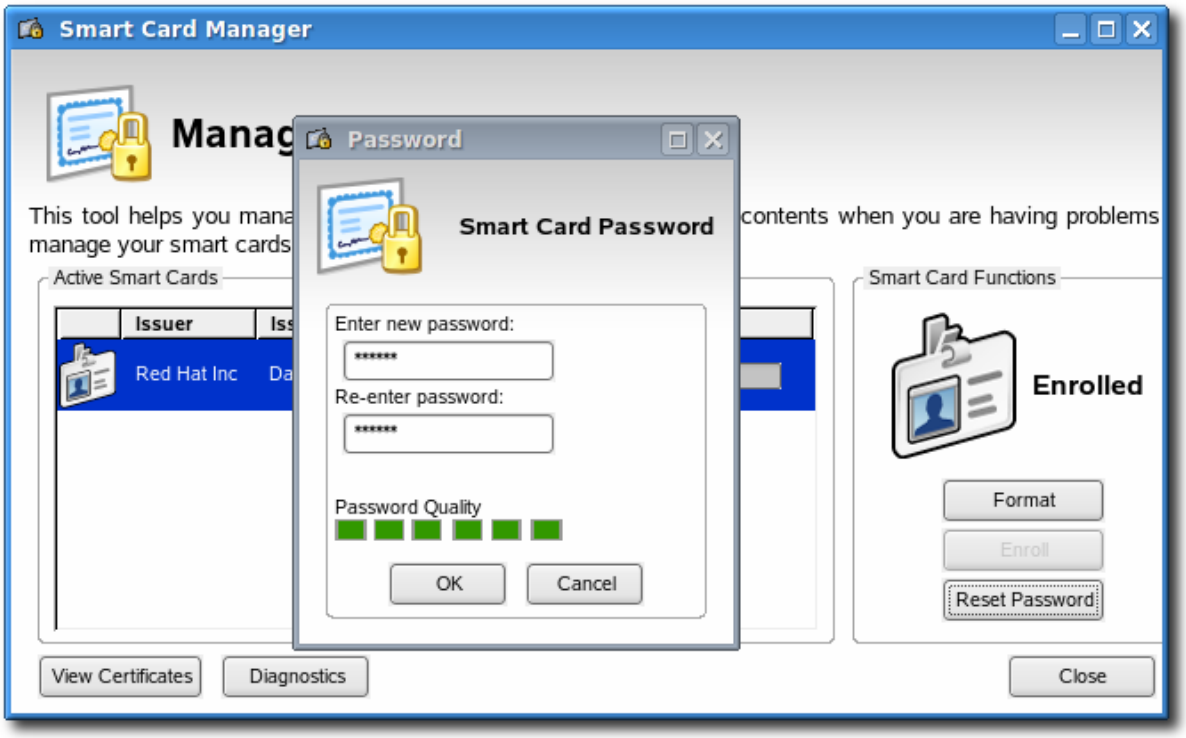
1. 在计算机上插入受支持的智能卡。确定在 **Active Smart Cards** 表中列出了该卡。
2. 在 **Manage Smart Cards 屏幕的 Smart Card Function** 部分中，单击 **Format**。
3. 如果为用户身份验证配置了 TPS，请在身份验证对话框中输入用户凭据，然后单击 **Submit**。
4. 在格式化过程中，卡的状态将变为 BUSY，并显示进度条。格式化过程完成后会显示成功信息。单击 **OK** 以关闭消息框。
5. 格式化过程完成后，**活动目录智能卡** 表会显示卡状态为 UNINITIALIZED。

3.5.2. 重置智能卡密码

如果用户在注册卡后忘记智能卡的密码，则可以重置密码。在智能卡中重置密码：

1. 在计算机上插入受支持的智能卡。确定在 **Active Smart Cards** 表中列出了该卡。
2. 在 Manage **Smart Cards 屏幕的 Smart Card Function** 部分中，单击 **Reset Password** 以显示 **Password** 对话框。
3. 在 Enter new password 字段中输入 **一个新的智能卡密码**。

4. 确认 **Re-Enter password** 字段中的新的智能卡密码，然后单击 **OK**。



5. 如果为用户身份验证配置了 TPS，请在身份验证对话框中输入用户凭据，然后单击 **Submit**。

6. 等待密码完成重置。

3.5.3. 查看证书

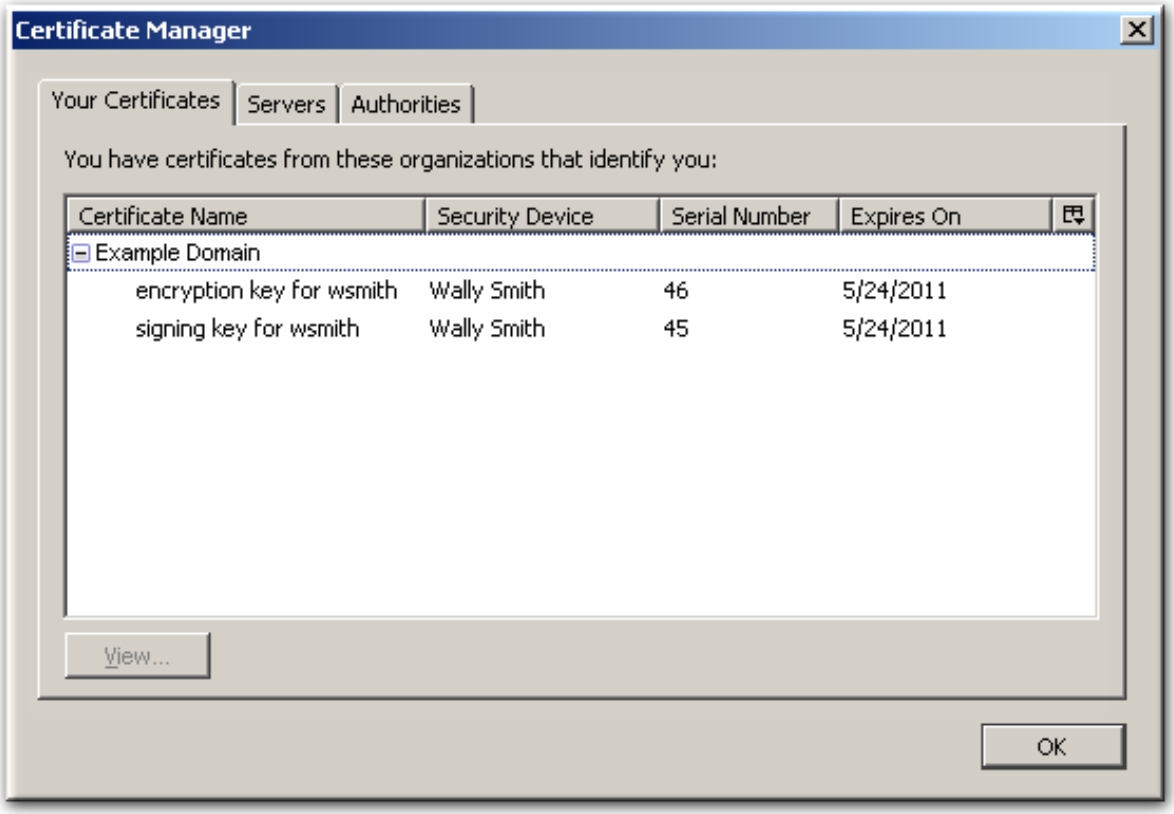
智能卡管理器 可以显示所选智能卡的基本信息，包括存储的密钥和证书。查看证书信息：

1. 在计算机上插入受支持的智能卡。确定在 **Active Smart Cards** 表中列出了该卡。

2. 从列表中选择卡，然后单击 **View Certificates**。

这将显示保存在卡中的证书的基本信息，包括序列号、证书别名和有效期日期。

3. 要查看证书的更多详细信息，请从列表中选择证书，然后单击 **View**。



3.5.4. 注册智能卡

大多数智能卡都将使用自动注册过程自动注册。您还可以使用 **管理智能卡** 工具手动注册智能卡。

如果您使用用户密钥对注册令牌，则令牌可用于基于证书的操作，如 SSL 客户端身份验证和 S/MIME。

注意

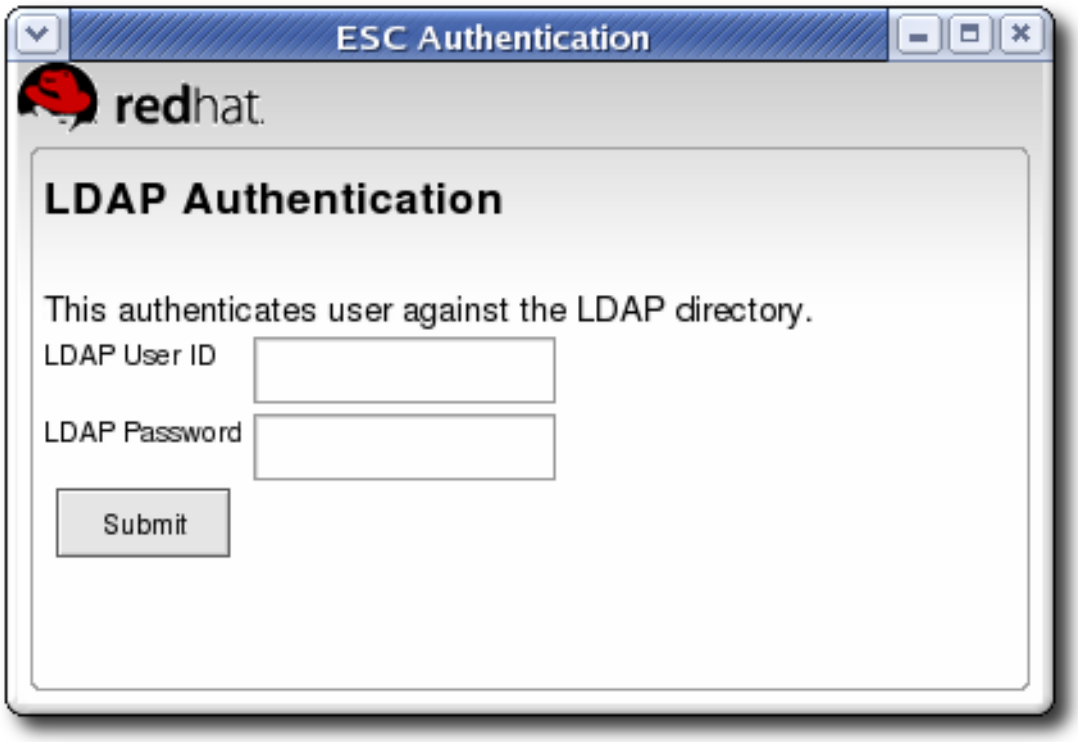
可将 TPS 服务器配置为在服务器上生成用户密钥对，然后在 DRM 子系统中归档，以便在令牌丢失时进行恢复。

手动注册智能卡：

1. 将受支持的、未注册的智能卡插入到计算机中。确定在 **Active Smart Cards** 表中列出了该卡。
2. 单击 **Enroll** 以显示 **密码** 对话框。
3. 在 **Enter a password** 字段中输入一个新密钥密码。

   在 **Re-Enter a password** 字段中确认新密码。
4. 单击 **OK** 以开始注册。
5. 如果为用户身份验证配置了 TPS，请在身份验证对话框中输入用户凭据，然后单击 **Submit**。

   如果 TPS 已配置为将密钥归档到 DRM，注册过程将开始生成和归档密钥。



注册完成后，智能卡的状态会显示为 ENROLLED。

3.6. 诊断问题

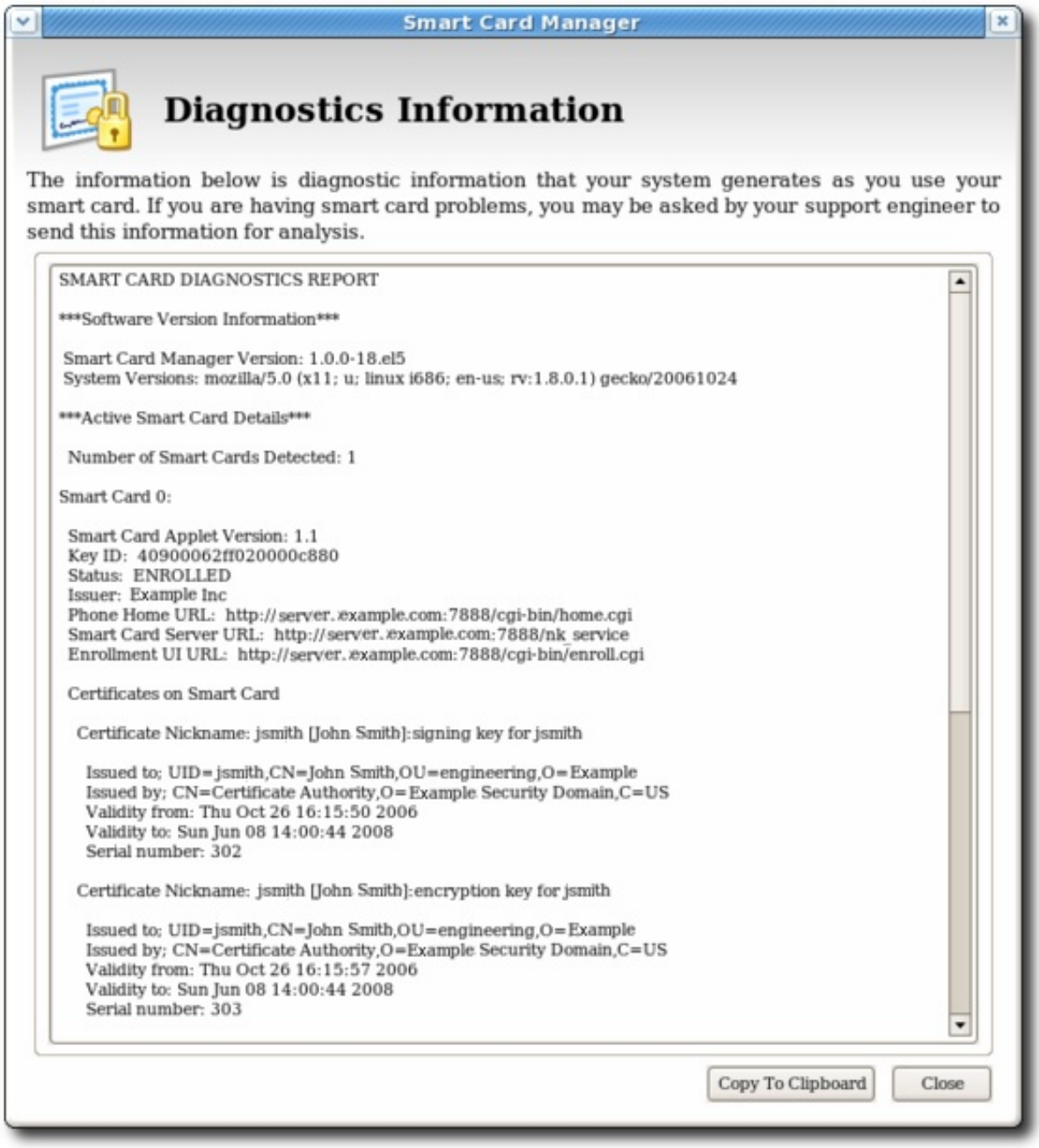
企业安全客户端包含基本的诊断工具和一个简单的接口，用于记录错误和常见事件，如插入和删除智能卡或更改卡的密码。诊断工具可以识别并通知用户有关企业安全客户端、智能卡和 TPS 连接的问题。

打开 过**期信息** 窗口：

1. 打开企业安全客户端。

2. 从列表中选择要检查的智能卡。
3. 点 **Diagnostics** 按钮。

4. 这会打开所选智能卡的附件 **信息** 窗口。



locateds Information 屏幕显示以下信息：

- 企业安全客户端版本号。
- 企业安全客户端检测到的卡数。

对于检测到的每个卡，会显示以下信息：

- 在智能卡上运行的 applet 版本。
- 智能卡的字母数字 ID。
- 卡的状态可以是三项：
  - *NO_APPLET* No key 被检测到。
  - *未初始化。*密钥已被检测到，但没有注册证书。
  - *已注册。*检测到的卡已使用证书和密钥信息注册。

- 卡的 phone Home URL。这是从中获取所有附件主页信息的 URL。
- 卡签发者名称，如 **示例公司。**
- 卡的回答到重设(ATR)字符串。这是一个唯一值，可用于识别不同类型的智能卡。例如：

  ```
  3BEC00FF8131FE45A0000000563333304A330600A1
  ```

- TPS Phone Home URL。
- TPS 服务器 URL。这通过 phone Home 检索。
- TPS 注册表单 URL。这通过 phone Home 检索。
- 有关卡中包含的每个证书的详细信息。
- 最新企业安全客户端错误和常见事件的运行日志。

企业安全客户端记录了两种类型的诊断信息。它记录了智能卡返回的 *错误*，并记录通过企业安全客户端发生的事件。*它还返回有关智能卡配置的基本信息。*

3.6.1. 错误

- *企业安全客户端无法识别卡。*
- *在智能卡操作过程中出现问题，如证书注册、密码重置或格式操作。*
- *企业安全客户端丢失了与智能卡的连接。当问题与 **PCSC** 守护进程通信时，可能会发生这种情况。*
- *企业安全客户端和 TPS 之间的连接丢失。*

*智能卡可向 TPS 报告某些错误代码；它们记录在 TPS 的 **tps-debug.log** 或 **tps-error.log** 文件中，具体取决于消息的原因。*

表 3.1. 智能卡错误代码

返回码	描述
常规错误代码	
6400	没有特定的诊断
6700	Lc 中错误的长度
6982	未满足安全性状态
6985	不满意的使用条件
6a86	P1 P2 不正确
6d00	无效的指令

返回码	描述
6e00	无效的类
安装负载错误	
6581	内存故障
6a80	data 字段中的参数不正确
6a84	没有足够的内存空间
6a88	未找到引用的数据
删除错误	
6200	应用程序已逻辑删除
6581	内存故障
6985	无法删除引用的数据
6a88	未找到引用的数据
6a82	未找到应用程序
6a80	命令数据中的不正确的值
获取数据错误	
6a88	未找到引用的数据
获取状态错误	
6310	更多可用数据
6a88	未找到引用的数据
6a80	命令数据中的不正确的值
加载错误	
6581	内存故障
6a84	没有足够的内存空间
6a86	P1/P2 不正确

返回码	描述
6985	不满意的使用条件

3.6.2. 事件

- 简单的事件，如卡插入和删除、成功完成的操作、导致错误以及类似的事件。
- 从 TPS 报告错误到企业安全客户端。
- NSS 加密库已初始化。
- 检测到其他低级智能卡事件。

第 4 章 将智能卡用于 WEB 和邮件客户端

注册智能卡后，智能卡可用于 SSL 客户端身份验证和 S/MIME 电子邮件应用程序。PKCS the 模块有不同的名称，并位于不同的目录中，具体取决于操作系统。

表 4.1. PKCS这个模块位置

平台	模块名称	位置
Red Hat Enterprise Linux	onepin-opensc-pkcs11.so	/usr/lib64/

4.1. 设置浏览器以支持令牌的 SSL

设置 Firefox 浏览器以支持令牌的 SSL ：

1. *打开 **编辑** 菜单并选择 **Preferences**。*

   *如果菜单栏在 Firefox 中不可见，请按 **Alt** 键临时显示它。*

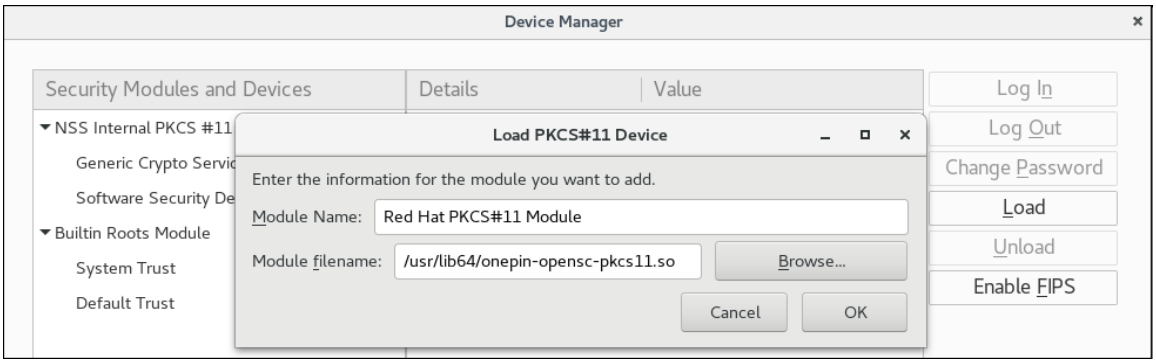
2. *在 **Advanced** 条目中，选择 **Certificates** 选项卡，然后单击 **Security Devices** 按钮。*

3. *添加 PKCS the 驱动程序：*

   a. *点 **Load** 按钮。*

   b. *输入模块名称。*

   c. *点 **Browse**，选择 Enterprise Security Client PKCS the driver 库，然后点 **OK**。*



4. *如果 CA 尚未被信任，请下载并导入 CA 证书。*

   1. *打开 CA 上的 **SSL End Entity** 页面。例如：*

      > *https://server.example.com:9444/ca/ee/ca/*

   2. *单击 **Retrieval** 选项卡，然后单击 **Import CA Certificate Chain**。*

   3. ***以二进制形式点 Download the CA certificate chain**，然后点 **Submit**。*

   4. *选择一个合适的目录来保存证书链，然后单击 **OK**。*

   5. *点击 **Edit > Preferences**，然后选择 **Advanced** 选项卡。*

6. 单击 **View Certificates** 按钮。
7. 单击 **Authorities**，然后导入 CA 证书。

5. 设置证书信任关系。
   1. 点击 **Edit > Preferences**，然后选择 **Advanced** 选项卡。
   2. 单击 **View Certificates** 按钮。
   3. 单击 **Edit**，再为网站设置信任。

证书可用于 SSL。

第 5 章 设置企业级安全客户端

注意

可以在无需额外配置的情况下启动企业安全客户端。

5.1. 为令牌操作禁用 LDAP 身份验证

默认情况下，请求令牌操作的每个用户都针对 LDAP 目录进行身份验证。如果用户有一个条目，则允许操作；如果用户没有条目，则拒绝操作。

出于测试目的或某些类型的用户，可以很简单或首选地禁用 LDAP 身份验证。这没有在企业安全客户端配置中进行配置，而是在令牌处理系统配置中进行配置，且必须由 TPS 管理员完成。

1. 停止 TPS 子系统。

```
# systemctl stop pki-tps
```

2. 打开 TPS 配置文件。

```
# vim /var/lib/pki-tps/conf/CS.cfg
```

3. 将身份验证参数设置为 **false**。

```
op.operation_type.token_type.loginRequest.enable=false
op.operation_type.token_type.auth.enable=false
```

operation_type 是禁用 LDAP 身份验证的令牌操作，如 **注册**、**格式** 或 **pinreset**。禁用一个操作类型的身份验证不会为任何其他操作类型禁用它。

token_type 是令牌配置集。常规用户、安全官以及由安全官注册的用户有默认配置文件。对于其他类型的用户或证书，也可以有自定义令牌类型。

例如：

```
op.enroll.userKey.loginRequest.enable=false
op.enroll.userKey.pinReset.enable=false
```

4. 重新启动 TPS 子系统。

```
# systemctl restart pki-tomcatd@pki-tomcat.service
```

Red Hat Certificate System 10 Administration Guide 中介绍了编辑 TPS 配置。

附录 A. 修订历史记录

请注意，修订号与该手册版本相关，而不是 Red Hat Certificate System 的版本号。

修订 10.1-0 **Fri Nov 20 2020** **Florian Delehaye**

发布 Red Hat Certificate System 10.1 指南。