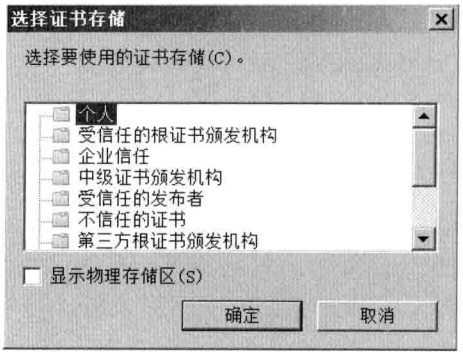

图 13-7　导入证书时手工选择证书存储位置

按照提示依次单击“下一步”按钮，将会成功导入证书到 Windows 证书库。

13.3.3　导出证书

在证书库查看界面中（见图 13-2），选择某证书后单击“导出”按钮，即进入证书导出向导。

首先，选择“您想将私钥跟证书一起导出吗？”，如图 13-8 所示。

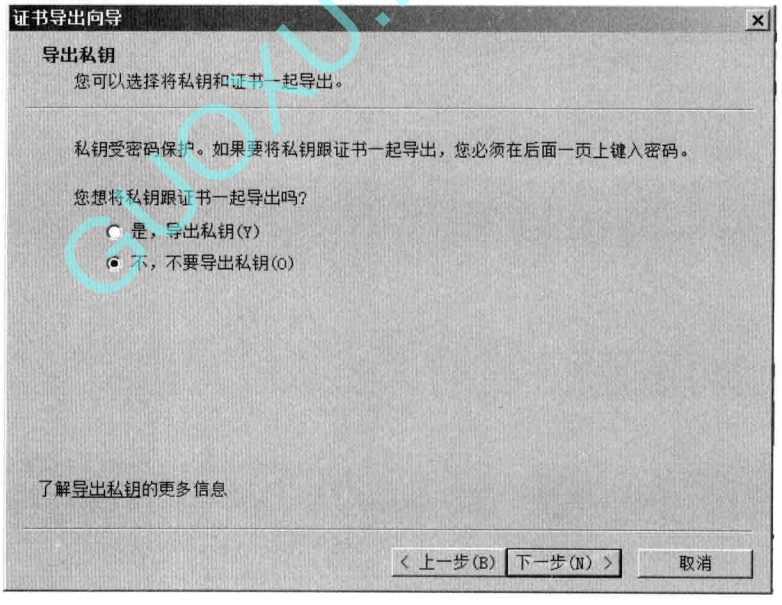

图 13-8　导出证书时选择是否导出私钥

然后，选择导出文件格式，如图 13-9 所示。支持的证书文件格式包括 PKCS#12（P12 或 PFX）、PKCS#7（P7B）、DER 编码二进制 X.509（CER）、Base64 编码 X。509（CER，文本格式）等。

最后，选择需要保存的证书文件名称，如图 13-10 所示。

按照提示依次单击“下一步”按钮，将会成功从 Windows 证书库导出指定证书。

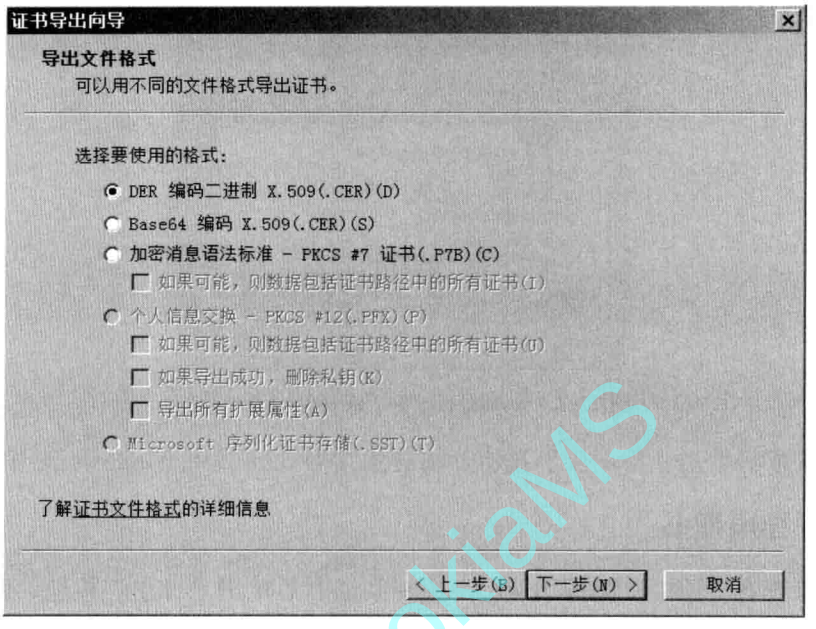

图 13-9　导出证书时选择文件格式

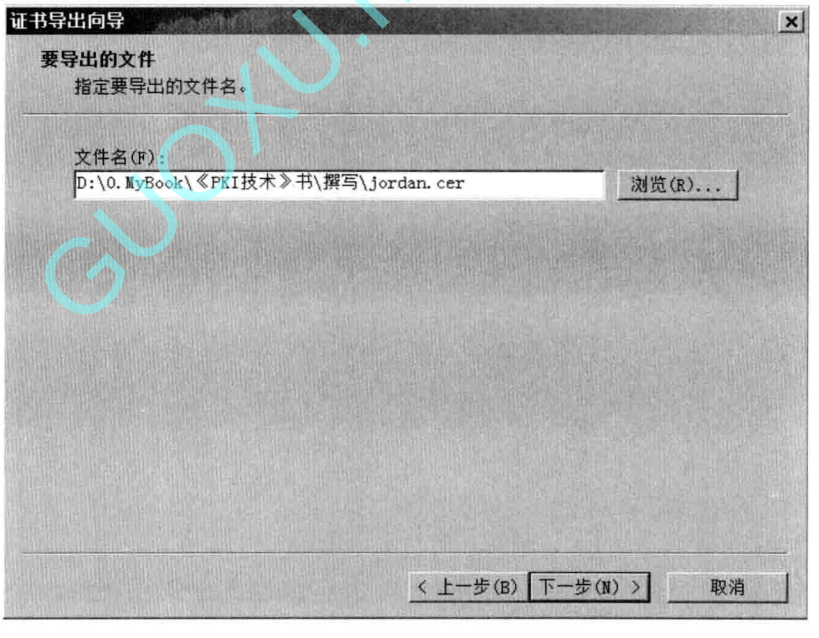

图 13-10　导出证书时选择证书文件名称

第四部分

PKI之CA与KMC：管理网络身份证

第14章 系统结构

14.1 国际标准

IETF RFC 3280 规定了 CA 的系统结构，其相关实体及其关系如图 14-1 所示。

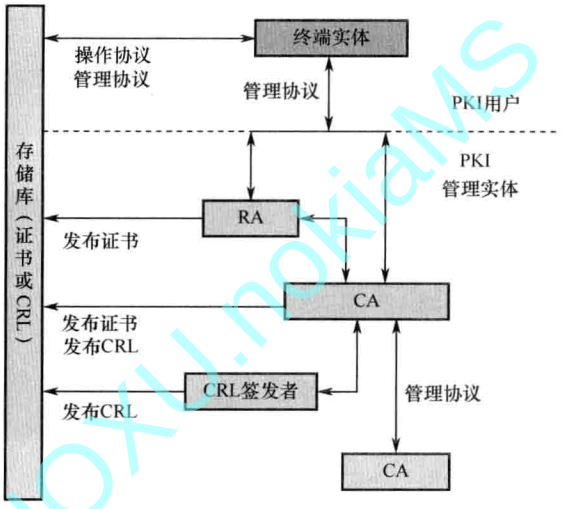

图 14-1 CA 相关实体及其关系

1. CA 相关实体（Entities）

① 终端实体（End Entity）：指应用环境中涉及他人证书的用户（user），或证书持有者 subject。

② CA：Certification Authority 的缩写，负责签发证书和 CRL，并将证书和 CRL 发布到存储库中。CA 支持多级，上级 CA 可以签发下级 CA，最下级 CA 只能签发终端实体证书，最顶级 CA 称作根 CA。为实现互联互通，不同 CA 之间可以签发交叉认证证书。

③ RA：Registration Authority 的缩写，属于可选系统。CA 可将部分管理功能授权给 RA 负责，如注册申请、证书发布等。

④ CRL 签发者（CRL Issuer）：属于可选系统。CA 可将 CRL 签发和 CRL 发布功能授权给 CRL 签发者负责。CRL 是 Certificate Revocation List 的缩写，表示证书作废列表。

⑤ 存储库（Repository）：分布式系统的统称，专门用于存储证书和 CRL。终端实体可以通过访问存储库而方便地获得所需的证书和 CRL。由于数字证书具有防伪性和有效期，因此数字证书可以通过任意非信任的系统进行分发，也可以存储到任何非安全的设备中。

2. 证书作废（Revocation）

数字证书签发后，在其有效期内应该处于有效状态。但是，有很多原因可能会导致处

于有效期内的证书不能继续使用，如名称发生改变、CA 和证书持有者 subject 之间的关系发生变化（如员工可能离职）、私钥泄露或被怀疑泄露。如果发生这些情况，CA 需要将该证书作废，使该证书处于无效状态。

CA 引入 CRL 机制用于对外发布作废证书。CRL 是 Certificate Revocation List 的缩写，表示证书作废列表。CRL 跟数字证书类似，是一个特殊的数据结构，由 CA 或 CRL 签发者签名、所有作废证书的序列号等组成，可以以文件形式存在。当应用系统接收到对方证书时，为验证该证书是否有效，不仅需要核对该证书中包含的 CA 签名和有效期，而且需要核对该证书是否已经作废（获取最新 CRL，检查该证书序列号是否在该 CRL 中）。CA 或 CRL 签发者定期签发并发布 CRL，并在 CRL 中指明下次签发的最晚时间。

由于 CRL 也具有防伪性，因此 CRL 也可以跟数字证书类似，通过任意非信任的系统进行分发。

3．操作协议（Operational Protocols）

操作协议用于将证书和 CRL（或状态信息）传递给客户端系统。可采用多种方式进行传递，如 LDAP、HTTP、FTP、X.500 等。

4．管理协议（Management Protocols）

管理协议用于 PKI 用户和管理实体之间进行功能交互。管理协议主要包括如下功能集合。

① 注册（Registration）：用户将用于申请证书的相关信息提交给 CA。可直接提交，也可通过 RA 间接提交。

② 初始化（Initialization）：为保证客户端系统运行时的安全性，在使用前需要预先正确地安装与密钥相关数据。例如，受信任 CA 的相关信息，以及用户自己的公/私钥对。

③ 签发证书（Certification）：CA 为用户公钥签发数字证书，并将证书返回给用户的客户端系统，同时将证书发布到存储库。

④ 密钥对恢复（Key Pair Recovery）：如果有需要，CA 或密钥备份系统可以备份用户的密钥资料（如私钥）。必要时，可为用户恢复密钥资料，如私钥、口令等。

⑤ 密钥对更新（Key Pair Update）：所有的密钥对都需要定期更新成新密钥对，然后签发新证书。

⑥ 作废请求（Revocation Request）：当证书出现异常时，用户可向 CA 提出申请，将该证书作废。

⑦ 交叉认证（Cross-Certification）：两个 CA 通过互相签发交叉认证证书实现互联互通。

14.2　国内标准

《证书认证系统密码及其相关安全技术规范》定义了 CA 与 KMC 的系统结构。该规范中将 CA 称作证书认证系统，KMC 称作密钥管理系统。KMC 只用于实现双证书机制（签名证书和加密证书）。

14.2.1　证书认证系统 CA

证书认证系统是对生命周期内的数字证书进行全过程管理的安全系统。证书认证系统