在逻辑上可分为核心层、管理层和服务层，具体包括：

① 核心层：由证书/CRL 签发系统、证书/CRL 存储发布系统构成。

② 管理层：由证书管理系统、安全管理系统构成。

③ 服务层：由用户注册管理系统（包括远程用户注册管理系统）、证书/CRL 查询系统构成。其中用户注册管理系统等价于 RA。

证书认证系统的结构如图 14-2 所示。

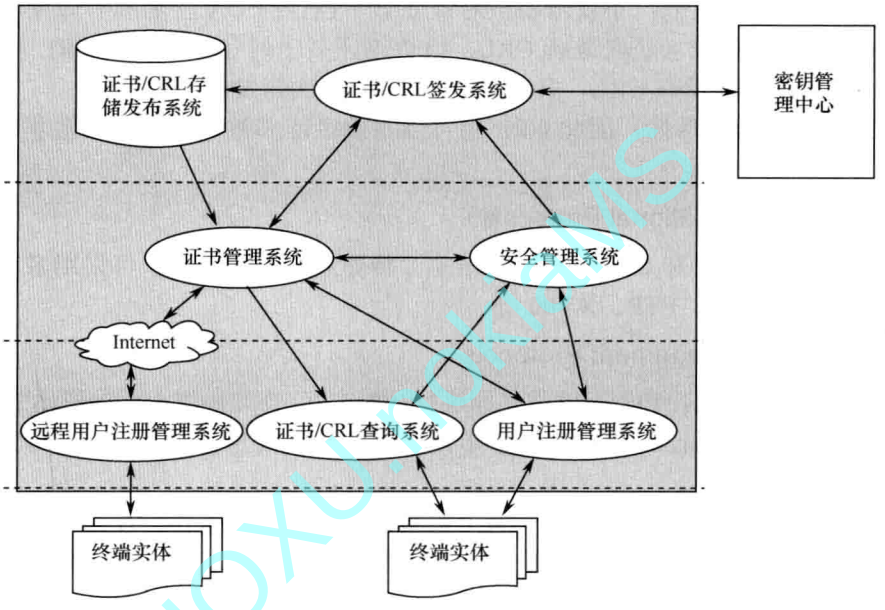

图 14-2　证书认证系统结构

1. 用户注册管理系统

用户注册管理系统负责用户的证书申请、身份审核和证书下载，可分为本地注册管理系统和远程注册管理系统。

（1）证书申请

证书申请可采用在线或离线两种方式。在线方式是指，用户通过互联网等登录到用户注册管理系统申请证书；离线方式是指，用户到指定的注册机构申请证书。

（2）身份审核

审核人员通过用户注册管理系统，对证书申请者进行身份审核。

（3）证书下载

证书下载可采用在线或离线两种方式。在线方式是指，用户通过互联网等登录到用户注册管理系统下载证书；离线方式是指，用户到指定的注册机构下载证书。

2. 证书/CRL 签发系统

证书/CRL 签发系统负责生成、签发数字证书和 CRL。

（1）证书类型

按主体对象，证书通常可分为人员证书、设备证书和机构证书 3 种类型。按功能，证

书可分为加密证书和签名证书两种类型。具体证书分类方式可根据实际需求进行设计。

（2）证书机制

当采用双证书机制时，每个用户拥有两张数字证书：一张用于数字签名，另一张用于信息加密。用于数字签名的密钥对可以由用户利用具有密码运算功能的证书载体产生；用于信息加密的密钥对由密钥管理系统产生。签名证书和加密证书一起保存在用户的证书载体中。

（3）证书签发

用户的数字证书由该系统的CA签发，根CA的数字证书由根CA自己签发，下级CA的数字证书由上级CA签发。

（4）CRL

CRL是在证书有效期之内，CA签发的终止使用证书的信息，分为用户证书作废列表（CRL）和CA证书作废列表（ARL）两类。在证书的使用过程中，应用系统通过检查CRL/ARL，获取有关证书的状态。

3．证书/CRL存储发布系统

证书/CRL存储发布系统负责数字证书、CRL的存储和发布。

根据应用环境的不同，证书/CRL存储发布系统可采用数据库或目录服务方式，实现数字证书/CRL的存储、备份和恢复等功能，并提供查询服务。

使用目录服务方式，可采用主、从目录结构以保证主目录服务器的安全。同时从目录服务器可以采用分布式的方式进行设置，以提高系统的效率。用户只能访问从目录服务器。

4．证书/CRL查询系统

证书/CRL查询系统负责为用户和应用系统提供证书状态查询服务，包括：

① CRL查询：用户或应用系统利用数字证书中标识的CRL地址，下载CRL，并检验证书的有效性。

② 在线证书状态查询：用户或应用系统按照OCSP协议，实时在线查询证书的状态。

在实际应用中，可以根据具体情况采用上述两种查询方式之一或全部。

5．证书管理系统

证书管理系统是证书认证系统中实现对证书/CRL的申请、审核、生成、签发、存储、发布、作废、归档等功能的管理控制系统。

6．安全管理系统

安全管理系统主要包括安全审计系统和安全防护系统。

安全审计系统提供事件级审计功能，对涉及系统安全的行为、人员、时间等记录进行跟踪、统计和分析。

安全防护系统提供访问控制、入侵检测、漏洞扫描、病毒防治等网络安全功能。

14.2.2 密钥管理系统KMC

密钥管理系统提供了对生命周期内的加密证书密钥对进行全过程管理的功能，包括密钥生成、密钥存储、密钥分发、密钥备份、密钥更新、密钥撤销、密钥归档、密钥恢复以

及安全管理等。

密钥管理系统的结构如图 14-3 所示。

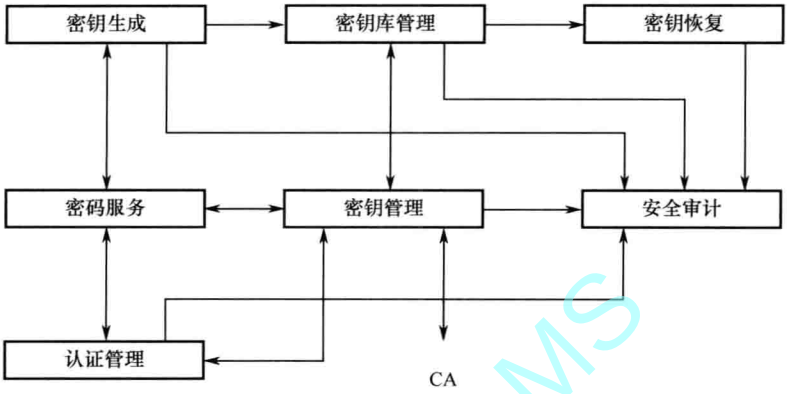

图 14-3　密钥管理系统结构

1．密钥生成

根据 CA 的请求为用户生成非对称密钥对（公私钥对），该密钥对应该由密钥管理系统的硬件密码设备生成。

2．密钥存储

密钥管理系统生成的非对称密钥对，经硬件密码设备加密后存储在数据库中。

3．密钥分发

密钥管理系统生成的非对称密钥对通过证书认证系统分发到用户证书载体中。

4．密钥备份

密钥管理系统采用热备份、冷备份和异地备份等措施实现密钥备份。

5．密钥更新

当证书到期或用户需要时，密钥管理系统根据 CA 请求为用户生成新的非对称密钥对。

6．密钥撤销

当证书到期、用户需要或管理机构认为必要时，密钥管理系统根据 CA 请求撤销用户当前使用的密钥。

7．密钥归档

密钥管理系统为到期或撤销的密钥提供安全的长期存储。

8．密钥恢复

密钥管理系统可为用户提供密钥恢复服务和为司法取证提供密钥恢复服务。密钥恢复需按管理策略进行审批，一般用户只限于恢复自身密钥。

第15章 系统设计

系统设计包括系统的整体设计和各子系统设计，《证书认证系统密码及其相关安全技术规范》定义了 CA 与 KMC 系统的设计原则和各子系统的实现方式。在具体实现过程中，应根据所选择的开发平台和开发环境进行详细设计。

15.1 证书认证系统 CA

证书认证系统应遵循以下总体设计原则：

① 证书认证系统遵循标准化、模块化设计原则。

② 证书认证系统设置相对独立的功能模块，通过各模块之间的安全连接，实现各项功能。

③ 各模块之间的通信采用基于身份验证机制的安全通信协议。

④ 各模块使用的密码运算都应该在密码设备中完成。

⑤ 各模块产生的审计日志文件采用统一的格式传递和存储。

⑥ 用户注册管理系统、证书/CRL 签发系统和密钥管理系统可以设置独立的数据库。

⑦ 系统必须具备访问控制功能。

⑧ 系统在实现证书管理功能的同时，必须充分考虑系统本身的安全性。

15.1.1 用户注册管理系统 RA

1. 系统功能

用户注册管理系统负责用户证书/CRL 的申请、审核以及证书的制作，其主要功能如下。

（1）用户信息的录入

录入用户的申请信息。用户申请信息包括签发证书所需要的信息，还包括用于验证用户身份的信息，这些信息存放在用户注册管理系统的数据库中。用户注册管理系统应能够批量接受从外部系统生成的、以电子文档方式存储的用户信息。

（2）用户信息的审核

提取用户的申请信息，审核用户的真实身份，当审核通过后，将证书签发所需要的信息提交给签发系统。

（3）用户证书下载

用户注册管理系统提供证书下载功能，当签发系统为用户签发证书后，用户注册管理系统能够下载用户证书，并将用户证书写入指定的用户证书载体中，然后分发给用户。

（4）安全审计

负责对用户注册管理系统的管理人员、操作人员的操作日志进行查询、统计以及报表打印等。

（5）安全管理

对用户注册管理系统的登录进行安全访问控制，并对用户信息数据库进行管理和备份。

（6）多级审核

用户注册管理系统可根据需要采用分级部署的模式，对不同种类和等级的证书，可由不同级别的用户注册管理系统进行审核。用户注册管理系统应能够根据需求支持多级注册管理系统的建立和多级审核模式。

用户注册管理系统应具有并行处理的能力。

2．模块组成

用户注册管理系统由本地注册管理、远程注册管理、数据库、信息录入、身份审核、证书制作、安全管理及安全审计几部分构成，其逻辑结构如图 15-1 所示。

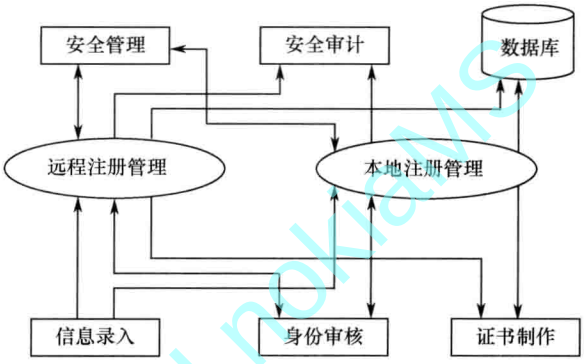

图 15-1　用户注册管理系统的逻辑结构

15.1.2　证书/CRL 签发系统

15.1.2.1　系统功能

证书/CRL 签发系统是证书认证系统的核心，不仅为整个证书认证系统提供签发证书/CRL 的服务，还承担整个证书认证系统中主要的安全管理工作。其主要功能如下。

（1）证书生成与签发

从数据库中读取用户信息，根据拟签发的证书类型向密钥管理系统申请加密密钥对，生成用户的签名证书和加密证书，将签发完成的证书发布到目录服务器和数据库中。根据系统的配置和管理策略，不同种类或用途的证书可以采用不同的签名密钥。

（2）证书更新

系统应提供 CA 证书及用户证书的更新功能。

（3）CRL 生成与签发

接收作废信息，验证作废信息中的签名，然后签发 CRL，将签发后的 CRL 发布到数据库或目录服务器中。签发 CRL 的签名密钥可以与签发证书的签名密钥相同或不同。

（4）安全审计

负责对证书/CRL 生成与签发系统的管理人员、操作人员的操作日志进行查询、统计以及报表打印等。

（5）安全管理

对证书/CRL 生成与签发系统的登录进行安全访问控制，并对证书/CRL 数据库进行管理和备份；设置管理员、操作员，并为这些人员申请和下载数字证书；配置不同的密码设