备；配置不同的证书模板。

证书/CRL 生成与签发系统应具有并行处理的能力。

15.1.2.2　模块组成

证书/CRL 签发系统由证书/CRL 生成与签发、安全管理、安全审计、数据库、目录服务器以及密码设备等组成。

1．证书/CRL 生成与签发

主要功能包括证书的生成与签发和 CRL/ARL 的生成与签发。

（1）证书的签发

根据接收的请求信息，从数据库中提取用户的信息，向密钥管理系统申请加密密钥对，然后生成并签发签名证书和加密证书，签发的证书和加密证书的私钥通过证书管理系统下传给申请者，同时将证书发布到数据库和目录服务器中。在此过程中，必须保证私钥传递的安全。

（2）CRL 的签发

首先验证申请信息中的数字签名，然后签发 CRL，并将 CRL 发布到数据库或目录服务器指定的位置。

2．密码设备

密码设备完成签名以及验证工作，并负责与其他系统通信过程中的密码运算，CA 的签名密钥保存在密码设备中。在进行上述工作时，必须保证所使用的密钥不能以明文形式被读出密码设备。

3．安全管理

安全管理主要包括以下内容。

① 证书模板配置：不同的证书种类由不同的证书模板确定，证书模板包括相应种类证书的基本项和证书的扩展项。

② CRL 发布策略配置：配置 CRL 的发布策略，包括自动/人工发布模式选择、发布时间间隔。

③ 进行 CA 密钥的更新。

④ 进行证书的备份和归档。

⑤ 进行服务器安全配置，包括服务器可接受的主机访问列表。

⑥ 为其他子系统定义管理员以及为这些管理员签发数字证书。

⑦ 数据库系统的配置：数据源的选择，数据库连接的用户名和口令设置。

4．安全审计

查询证书/CRL 生成与签发系统中的安全审计日志，并进行统计与打印。

15.1.3　证书/CRL 存储发布系统

1．系统功能

证书/CRL 存储发布系统负责证书和 CRL 的存储与发布，是证书认证系统的基础组成部分。证书的存储和发布必须采用数据库、目录服务器或其中之一。

该系统主要功能如下：

① 证书存储。

② CRL 存储。

③ 证书和 CRL 发布。

④ 安全审计：负责对证书/CRL 存储发布系统的管理人员、操作人员的操作日志进行查询、统计及报表打印等。

⑤ 安全管理：对证书/CRL 存储发布系统的登录进行访问控制，并定期对数据库和目录服务器进行管理和备份。

⑥ 数据一致性检验：对数据库和目录服务器中的数据进行一致性检验。

2．模块组成

证书/CRL 存储发布系统由数据库或主/从目录服务器、安全管理模块、安全审计模块组成。

（1）数据库

存放证书和 CRL 及用户的其他信息。

（2）目录服务器

证书/CRL 存储发布系统采用主从结构的目录服务器，签发完成的数据直接写入主目录服务器中，然后由目录服务器的主从映射功能自动映射到从目录服务器中。主从目录服务器通常配置在不同等级的安全区域，用户只能访问从目录服务器。

（3）安全管理

安全管理主要包括以下内容。

① 定期对数据库和目录服务器的内容进行数据备份和归档。

② 对数据库和目录服务器中的数据进行一致性检查，发现不一致时，应进行数据恢复。

（4）安全审计

查询证书/CRL 存储与发布系统中的安全审计日志，并进行统计与打印等。

15.1.4 证书/CRL 查询系统

1．系统功能

证书/CRL 查询系统为用户及应用系统提供证书状态查询服务，可以采用以下两种方式。

（1）CRL 查询

用户或应用系统利用证书中标识的 CRL 地址，查询并下载 CRL 到本地，进行证书状态的检验。

（2）在线证书状态查询

用户或应用系统利用 OCSP 协议，在线实时查询证书的状态，查询结果经过签名后返回给请求者，进行证书状态的检验。

2．模块组成

证书/CRL 查询系统由证书状态数据库/OCSP 服务器、安全管理模块、安全审计模块以及密码设备组成。

（1）证书状态数据库/OCSP 服务器

接受用户及应用系统的证书状态查询请求，根据请求信息中的证书序列号，从证书状

态数据库中查询证书的状态，并将查询结果返回给请求者。

（2）密码设备

验证请求信息中的签名，并对查询结果进行签名。

（3）安全管理

安全管理主要包括以下内容。

① OCSP 服务器的配置，定义可接受的访问控制信息以及查询的证书状态数据库的地址。

② 启动/停止查询服务，配置可接受的用户请求数量等。

（4）安全审计

查询证书状态查询系统中的安全审计日志，并进行统计与打印等。

15.1.5 证书管理系统

证书管理系统是证书认证系统的综合信息控制和调度服务系统，它接收用户的各种请求信息，并将请求信息提交给相应的子系统。

证书管理系统是一个逻辑上独立的系统，在进行系统设计过程中，可根据证书认证系统提供的服务，由不同的处理模块组成。这些模块可以采用分布式结构，以增强系统的处理能力，提高系统的效率。

15.1.6 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。

1. 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、时间的记录进行跟踪、统计和分析。安全审计系统可以分别查询各子系统中的日志记录，也可以通过查询证书/CRL 存储与发布系统中的数据库进行集中审计。

日志记录的主要内容包括：

① 操作员姓名。

② 操作项目。

③ 操作起始时间。

④ 操作终止时间。

⑤ 证书序列号。

⑥ 操作结果。

日志管理的主要内容包括：

① 日志参数设置。设置日志保存的最大规模和日志备份的目录。

② 日志查询。查询操作员、操作事件信息。

③ 日志备份。当日志保存到日志参数设置的最大规模时，将保存的日志备份。

④ 日志处理。对日志记录的正常业务流量和各类事件进行分类整理。

⑤ 证据管理。对证据数据进行审计、统计和记录。

2. 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。

15.2 密钥管理系统 KMC

密钥管理系统应遵循以下总体设计原则：

① 密钥管理系统遵循标准化、模块化设计原则。

② 密钥管理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必须在密码设备中完成。

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 系统必须具备访问控制功能。

⑦ 系统在实现密钥管理功能的同时，必须充分考虑系统本身的安全性。

⑧ 系统可为多个 CA 提供密钥服务。当为多个 CA 提供密钥服务时，由上级 CA 为密钥管理系统签发证书。

1. 密钥生成模块

密钥生成模块应提供以下主要功能：

① 非对称密钥对的生成，并将其保存在备用库中。当备用库中密钥数量不足时，自动进行补充。

② 对称密钥的生成。

③ 随机数的生成。

2. 密钥管理模块

密钥管理模块应提供以下主要功能：

① 接收、审核 CA 的密钥申请。

② 调用备用密钥库中的密钥对。

③ 向 CA 发送密钥对。

④ 对调用的备用密钥库中的密钥对进行处理，并将其转移到在用密钥库。

⑤ 对在用密钥库中的密钥进行定期检查，将超过有效期的或被撤销的密钥转移到历史密钥库。

⑥ 对历史密钥库中的密钥进行处理，将超过规定保留期的密钥转移到规定载体。

⑦ 接收与审查关于恢复密钥的申请，依据安全策略进行处理。

⑧ 对进入本系统的有关操作及操作人员进行身份与权限的认证。

3. 密钥库管理模块

密钥库管理模块负责密钥的存储管理，按照其存储的密钥的状态，密钥库分为备用库、在用库和历史库 3 种类型，密钥库中的密钥数据必须加密存放。

（1）备用库

备用库存放待使用的密钥对。密钥生成模块预生成一批密钥对，存放于备用库中；CA

需要时，可及时调出，将其提供给CA后转入在用库。

备用密钥库应保持一定数量的待用密钥对，存放的密钥数量依系统的用户数量而定，若少于设定的最低数量则应自动补足到规定数量。

（2）在用库

在用库存放当前使用的密钥对。在用库中的密钥记录包含用户证书的序列号、ID号和有效时间等标志。

（3）历史库

历史库存放过期或已被撤销的密钥对。历史库中的密钥记录包含用户证书的序列号、ID号有效时间和作废时间等标志。

4. 认证管理模块

认证管理模块负责对进入本系统的有关操作及操作人员进行身份与权限的认证。

5. 安全审计模块

安全审计模块负责各个功能模块的运行事件检查、有关资料分析和密钥申请统计等服务。审计项目主要包括：

① 运行事件记录。

② 服务器状态记录。

③ 系统重要策略设置。

审计记录不能进行修改。

6. 密钥恢复模块

密钥恢复模块负责为用户和司法取证恢复用户的加密私钥，被恢复的私钥必须安全地下载到载体。

（1）用户密钥恢复

用户通过RA申请，经审核后，由CA向密钥管理系统提出密钥恢复请求，密钥恢复模块恢复用户的密钥并通过CA返回RA，下载于用户证书载体中。

（2）司法取证密钥恢复

司法取证人员必须到KMC进行司法取证密钥恢复，KMC对司法取证人员的身份进行认证，认证通过后，由密钥恢复模块恢复所需的密钥并下载于特定载体中。

7. 密码服务模块

密码服务模块负责为密钥管理系统的各项业务提供密码支持。

密码服务模块配置经国家密码主管部门审批的非对称密钥密码算法、对称密钥密码算法和数据摘要算法等。

密码算法必须在硬件密码设备中运行。

8. 审计模块

密钥管理系统设置日志审计模块，包括全程审计和事件审计。审计员定时调出审计记录，制作统计分析表。审计员可以处理但不能修改日志审计数据。

日志记录的主要内容包括：

① 操作员姓名。