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。日志查询主要是查询操作员、认证机构操作事件信息。
③ 日志备份。当保存的日志达到参数设置的最大规模时，将对已有日志进行备份。
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。

15.3 企业级 CA 总体设计示例

从管理主体和服务对象分析，一般可将 CA 系统分为两类：运营型 CA 和企业级 CA。

运营型 CA 通常以第三方电子认证服务机构（CA 中心）方式存在，并由其运营和管理，提供具有法律效力的第三方电子认证服务，并承担相应的法律责任；不仅需要构建专业的 CA 机房和健全的法律文件，而且还需要确保 CA 系统和认证业务的安全性，同时还要满足物理环境与设施、组织与人员管理、文档/记录与介质管理、业务连续性、审计与改进、认证服务性能等方面的多种要求。运营型 CA 可以为多个行业的多种应用提供服务，具有很强的通用性和独立性；证书规模至少在几十万以上，投资规模也比较庞大。

企业级 CA 通常由企业内部特定部门或团队维护和管理，只是作为一类安全系统对待，只为该企业自身的 IT 系统提供应用安全服务，证书规模一般在几万以内，投资规模较小。企业级 CA 系统不仅需要同企业的各种应用进行深度融合，而且还需要适应组织内部的行政管理模式，在灵活部署、方便使用、易于扩展等方面要求较高。

本节主要介绍企业级 CA 系统总体设计的一种示例和实践，仅供参考。

15.3.1 技术路线选择

1. 通用性技术路线

① 管理 UI：采用 B/S 模式。

② 运营平台：操作系统优先使用 Linux，应支持多种操作系统；数据库优先使用 MySQL，应支持多种数据库，通过 JDBC 访问数据库；应用中间件优先使用 Tomcat。

③ 开发工具：前台模块优先使用 C、C++或 VC，如控件、客户端工具等；后台 Web 服务模块优先使用 JSP、Servlet 或 JDK。

2. 专业性技术路线

（1）证书机制

① 证书分类：分为个人、单位、Web、设备等，可扩展。
② 证书状态：包括正常、作废、冻结、解冻、过期等。

③ 证书业务状态：分为证书申请、证书作废、证书冻结、证书解冻、证书更新等。其中，证书申请状态包括已录入、审核通过、审核失败、已制作；证书作废状态包括已录入、审核通过、审核失败；证书冻结状态包括已录入、审核通过、审核失败；证书解冻状态包括已录入、审核通过、审核失败；证书更新状态包括已录入、审核通过、审核失败、已更新。

④ 证书申请流程：分为三步流程和一步流程两种。三步流程由录入、审核、制作组成，每步流程分别由不同业务员进行操作；一步流程由同一个业务员一次性完成。

⑤ 证书更新流程：分为三步流程、二步流程和一步流程 3 种。三步流程由录入、审核、更新组成，二步流程由审核（基于旧证书）、更新组成，每步流程分别由不同业务员进行操作；一步流程由同一个业务员一次性完成。证书制作时可通过旧证书对证书申请者进行身份认证。

⑥ 证书作废/冻结/解冻流程：分为二步流程和一步流程两种。二步流程由录入、审核、组成，每步流程分别由不同业务员进行操作；一步流程由同一个业务员一次性完成。

（2）管理机制

① 三级管理：分为 CA 管理员、RA 管理员、RA 操作员 3 级。

② 身份认证：支持证书模式和口令模式。

③ 访问控制：采用 RBAC 机制。

④ CA 管理员：主要职责是对 CA 进行管理，包括初始化、CA 策略管理、RA 管理、RA 管理员管理、查询统计、强制业务功能等。

⑤ RA 管理员：主要职责是对 RA 操作员进行管理。

⑥ RA 操作员：主要职责是进行具体业务操作，又分为 3 种角色：录入员、审核员、制作员。

具体管理机制如图 15-2 所示。

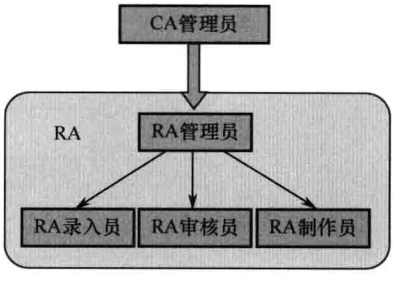

图 15-2　企业级 CA 管理机制

（3）RA 服务

① 业务功能：主要包括证书申请、证书作废、证书更新、证书冻结、RA 操作员管理、查询统计、RA 策略管理等。

② RA 管理员：主要职责包括操作员管理、查询统计、RA 策略配置、强制业务功能等。

③ RA 录入员：主要职责包括查询统计、录入等。

④ RA 审核员：主要职责包括查询统计、审核等。

⑤ RA 制作员：主要职责包括查询统计、制作等。

（4）证书服务

分为 Web 服务类和非 Web 服务类。

① Web 服务类：主要包括 CA 证书下载（支持证书链）、CRL 下载、单证书下载/更新、双证书下载/更新、Web 证书下载、证书查询、证书申请/更新自助录入、证书作废/冻结/解冻自助录入等。

② 非 Web 服务类：主要包括 OCSP/SOCSP 服务、LDAP 证书服务、证书验证服务等。

（5）安全性

① License 控制：通过证书数和 RA 数控制 License。

② Web 方式管理：身份认证优先采用证书认证方式（双向 SSL 或单向 SSL+安全控件），也可以支持口令方式。

③ 用户自助下载证书：采用口令方式进行身份认证。

④ 口令存储安全性：数据库中应该加密存储。

⑤ 关键数据存储完整性：采用 HMAC 机制。

⑥ 关键数据传输机密性：在 RA 与 CA 间采用对称加密机制。

15.3.2 模块设计

企业级 CA 系统模块组成如图 15-3 所示，其中以 w 开头的模块表示以 Web 方式提供服务。

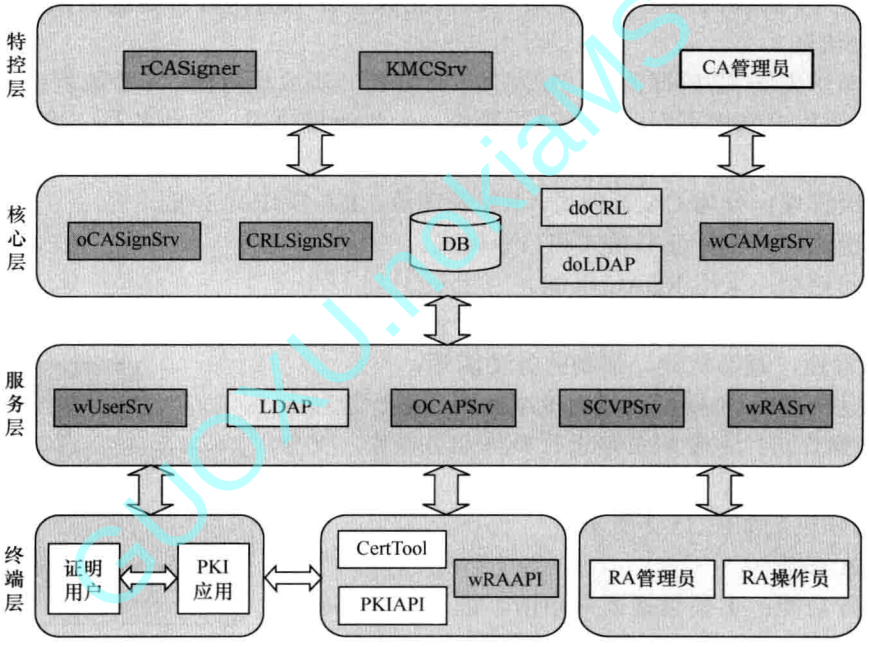

图 15-3 企业级 CA 系统模块组成

各模块主要功能如下。

① rCASigner：主要功能包括产生根 CA 公私钥对、签发根 CA 证书、签发运营 CA 证书、签发 CRL 签名者证书、支持软件 HSM 和硬件 HSM 等。

② KMCSrv：主要功能包括对外提供加密公私钥对产生服务、支持软件 HSM 和硬件 HSM 等。

③ oCASignSrv：主要功能包括产生运营 CA 公私钥对、对外提供证书签发服务、支持单证书和双证书签发、支持软件 HSM 和硬件 HSM、对外提供 License 验证服务等。

④ CRLSignSrv：主要功能包括产生 CRL 签名者公私钥对、对外提供 CRL 签发服务等。

⑤ wCAMgrSrv：主要功能包括配置 CA 参数、管理 RA、管理 CA 管理员和 RA 管理员、证书管理高级功能（强制申请、强制作废、强制冻结、强制解冻、强制审核、强制更新等）等。

⑥ doCRL：主要功能包括定时从数据库提取证书，并提交 CRLSignSrv 签名后，保存到数据库或文件中。

⑦ doLDAP：主要功能包括定时从数据库提取证书，发布到 LDAP 中。

⑧ DB：优先使用 MySQL。

⑨ wUserSrv：主要功能包括下载 CA 证书（根 CA、运营 CA）、下载 CRL、根据条件查询并下载他人证书、自身证书申请（产生公私钥对、提交 P10 包、安装证书等）、自身证书更新（通过旧证书进行身份认证）等。

⑩ LDAP：优先使用 OpenLDAP。

⑪ OCSPSrv：基于 OCSP（Online Certificate Status Protocol）协议提供在线证书状态查询服务。

⑫ SCVPSrv：基于 SCVP（Server-based Certificate Validation Protocol）协议提供在线证书验证服务。

⑬ wRASrv：主要功能包括管理 RA 操作员、证书管理普通功能（证书申请、证书作废、证书冻结、证书解冻、证书更新等）、证书管理高级功能（强制申请、强制作废、强制冻结、强制解冻、强制审核、强制更新等）等。

⑭ wRAAPI：对外提供 API 方式，方便将 RA 功能与应用系统集成，主要包括强制申请、强制作废、强制冻结、强制解冻、强制审核、强制更新等证书管理高级功能。

⑮ CertTool：主要功能包括查看证书信息、产生或拆分 P12 证书链、各种加密算法测试等。

各模块开发工具、依托资源和存储方式如表 15-1 所示。

表 15-1　企业级 CA 系统开发工具、依托资源和存储方式

/	模块名称	开发工具	依托资源	存储方式
1	rCASigner	Ansi C	openssl	文件系统
2	KMCSrv	Ansi C	openssl	文件系统
3	oCASignSrv	Ansi C	openssl	文件系统
4	CRLSignSrv	Ansi C	openssl	文件系统
5	wCAMgrSrv	Java	Tomcat+JRE+JDBC+MySQL	数据库
6	doCRL	Java	Tomcat+JRE+JDBC+MySQL	数据库
7	doLDAP	Java	Tomcat+JRE+JDBC+MySQL	数据库
8	DB	/	MySQL	数据库
9	wUserSrv	Java	Tomcat+JRE+JDBC+MySQL	数据库
10	LDAP	Java	LDAP	数据库
11	OCSPSrv	Java	Tomcat+JRE+JDBC+MySQL	数据库
12	SCVPSrv	Java	Tomcat+JRE+JDBC+MySQL	数据库
13	wRASrv	Java	Tomcat+JRE+JDBC+MySQL	数据库
14	wRAAPI	Java、Ansi C	/	待定
15	CertTool	VC++	openssl	/

15.3.3　数据库设计

数据库表设计如表 15-2 所示。

表 15-2　企业级 CA 数据库表

/	表名称	主要目的	/	表名称	主要目的
1	caconf	保存系统各种配置参数	5	userinfo	保存用户基本信息
2	rainfo	保存 RA 信息	6	userbiz	保存用户证书管理信息
3	opinfo	保存操作员信息	7	usercert	保存用户证书信息
4	loginfo	保存操作日志	8	cacrl	保存 CRL 信息

假设数据库名称、密码和用户暂时设置为 appca、appca 和 caadmin（可以修改）。数据库表结构设计如下：

```
drop database appca;
drop user caadmin;
create database appca;
use appca;
```

CREATE TABLE `caconf` (`confid` int NOT NULL, `confvalue` text NOT NULL, `confstatus` int NOT NULL, `remark` text DEFAULT NULL, PRIMARY KEY (`confid`)) ENGINE=InnoDB DEFAULT CHARSET=utf8;

CREATE TABLE `rainfo` (`raid` varchar(100) NOT NULL, `raname` varchar(100) NOT NULL, `racontactor` varchar(100) DEFAULT NULL, `ratel` varchar(100) DEFAULT NULL, `ramp` varchar(100) DEFAULT NULL, `raemail` varchar(100) DEFAULT NULL, `rastatus` int NOT NULL, `ranotbefore` varchar(25) DEFAULT NULL, `ranotafter` varchar(25) DEFAULT NULL, `macvalue` varchar(100) DEFAULT NULL, `fromtime` varchar(25) NOT NULL, `lasttime` varchar(100) NOT NULL, `lastopid` varchar(100) NOT NULL, `remark` text DEFAULT NULL, PRIMARY KEY (`raid`)) ENGINE=InnoDB DEFAULT CHARSET= utf8;

CREATE TABLE `opinfo` (`opid` varchar(100) NOT NULL, `op2raid` varchar(100) NOT NULL, `opname` varchar(100) NOT NULL, `oporg` varchar(100) DEFAULT NULL, `oporgunit` varchar(100) DEFAULT NULL, `oporgpos` varchar(100) DEFAULT NULL, `optel` varchar(100) DEFAULT NULL, `opmp` varchar(100) DEFAULT NULL, `opemail` varchar(100) DEFAULT NULL, `opstatus` int NOT NULL, `optype` int NOT NULL, `opauthtype` int NOT NULL, `opnotbefore` varchar(25) DEFAULT NULL, `opnotafter` varchar(25) DEFAULT NULL, `opcertsn` varchar(100) DEFAULT NULL, `opcertnotbefore` varchar(25) DEFAULT NULL, `opcertnotafter` varchar(25) DEFAULT NULL, `opcertvalue` text DEFAULT NULL, `opcerthash` varchar(100) DEFAULT NULL, `opcode` varchar(100) NOT NULL, `oppin` varchar(100) NOT NULL, `macvalue` varchar(100) DEFAULT NULL, `fromtime` varchar(25) NOT NULL, `lasttime` varchar(25) NOT NULL, `lastopid` varchar(100) NOT NULL, `remark` text DEFAULT NULL, PRIMARY KEY (`opid`)) ENGINE=InnoDB DEFAULT CHARSET=utf8;

CREATE TABLE `loginfo` (`logid` varchar(100) NOT NULL, `log2raid` varchar(100) NOT NULL, `logtype` int NOT NULL, `logresult` int NOT NULL, `logresultinfo` text DEFAULT NULL, `logsubjecttype` int NOT NULL, `logsubjectid` varchar(100) NOT NULL, `logsubjectinfo` text DEFAULT NULL, `logobjectid` varchar(100) DEFAULT NULL, `logobjectinfo` text DEFAULT NULL, `logtime` varchar(25) NOT NULL, `logopcertvalue` text DEFAULT NULL, `logopcertsign` text DEFAULT NULL, `macvalue` varchar(100) DEFAULT NULL, PRIMARY KEY (`logid`)) ENGINE=InnoDB DEFAULT CHARSET=utf8;

CREATE TABLE `userinfo` (`userid` varchar(100) NOT NULL, `user2raid` varchar(100) NOT NULL,