其中,通过证书模板来快速设计不同的证书产品,证书产品基于证书模板快速生成。 业务类型包括申请、作废等,其操作对象为证书产品。通过项目来管理不同的用户或行业 领域,基于项目对发证点进行业务授权。

### 2. 广义 RA 系统

除证书模板功能外,其他业务管理功能应该由 RA 来实现。传统的 RA 并不包括上述业务管理功能,只包括纯证书业务,即证书申请/补办/更新、证书作废、证书冻结/解冻、证书解锁等。为便于说明,本书将传统 RA 系统称为狭义 RA 系统,而将包含计费收费、档案管理、项目及产品管理、发证点管理、用户管理等功能的 RA 系统称为广义 RA 系统。

广义 RA 系统与 CA、KMC、应用系统等关联方的关系模型如图 25-2 所示,其中远程 RA 可以是广义 RA,也可以是狭义 RA。

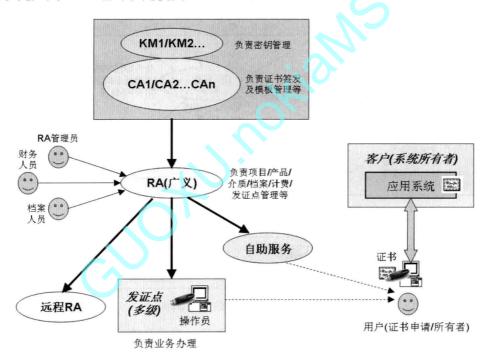


图 25-2 广义 RA 系统关联方模型图

考虑到以下几点原因, CA 中心可能会存在多套 CA 系统和 KMC 系统,不同类型证书可能由不同 CA 签发,而且不同系统可能采用不同厂商产品:

- ① 不同用户或行业领域的证书产品需要不同的密码算法。如 A 行业可能需要 RSA 1024 和 SHA1 算法, B 行业可能需要 RSA 2048 和 SHA1 算法, C 行业可能需要 SM2 和 SM3 算法。如电子政务证书和电子商务证书可能采用不同算法。
- ② 密码算法存在安全期,只在一定的时期内是安全的,超过安全期后,该密码算法就会被新的密码算法替代。如 RSA 1024 将被 RSA 2048 或 SM2 替代。
  - ③ 在市场竞争的影响下,有些系统厂商可能会被淘汰。 为适应或屏蔽多个 CA 系统的差异性,需要增加协议转换系统,负责协议转换(通信

及报文)、证书模板管理、RA 管理等功能。其中,RA 管理包括RA 服务器证书、允许的证书模块及证书数量等。RA 从协议转换系统下载证书模板,基于证书模块进行管理授权。

为实现多个 RA 情况下的用户统一管理,需要建设独立的用户管理系统,负责用户汇总、证书统计和分析、用户分析和挖掘等功能。其中,当 RA 分多级时,子 RA 需同时提交用户信息和证书信息,行业 RA 只需提交证书信息。

扩展上述功能后, CA 系统的系统结构将演变为如图 25-3 所示。

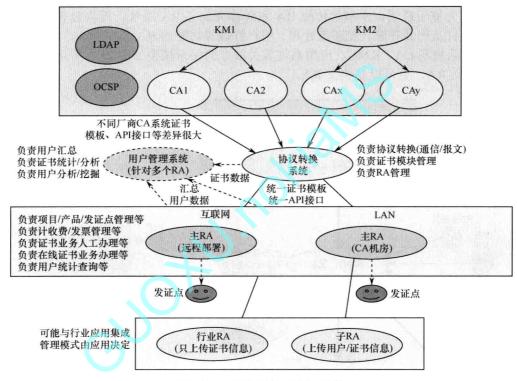


图 25-3 演变后 CA 的系统结构

因广义 RA 系统完成大部分业务管理功能,为进一步提高客户服务满意度,需要跟专业的客服系统实现互联互通。广义 RA 系统的系统结构如图 25-4 所示。

# 25.1.2 具体要求

#### 1. 证书模板

证书模板特指按照 X.509 证书格式框架,对某类证书格式中的各项内容进行预先定义的一种数据集合。

证书模板基本要求如下:

- ① 证书模板属于技术范畴,不属于业务范畴。
- ② 证书模板应由 CA 管理, 不允许 RA 修改。
- ③ 应能对证书模板进行授权: 授权给 RA。
- ④ 证书模板应包含运营 CA 系统或证书签发服务器、申请人算法、签名算法等;不同 CA 系统、不同申请者密钥算法、不同签名算法应使用不同的证书模板。

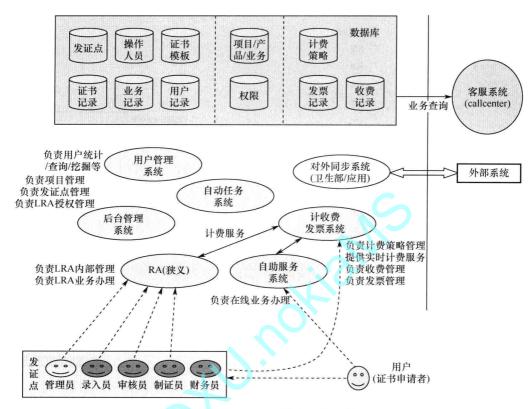


图 25-4 广义 RA 系统的系统结构

图 25-5 和图 25-6 给出了证书模板定义的一个实例,前者为基本项定义,后者为标准扩展项定义。



图 25-5 证书模板定义:基本项

AND THE RESIDENCE OF THE PARTY		
□ 颁发密钥标识符	<b>二</b> 关键	
厂 主题密钥标识符	厂 关键	
□ 颁发机构信息访问	□ 关键	
□ CRL发布点	厂 关键	
厂 证书策略	厂 关键	
□ 基本限制	□ 关键	
	□ CA	证书路径长度约束 -1
- 密钥用法	厂 关键	TO THE PERSON I
- 7 7 14 147	□ 数字签名	
	厂 不可否认	
	密钥加密	
	数据加密	
	密钥协商	
	证书签名	
	CRL签名	
	口 只用作加密	
	□ 只用作解密	
增强型密钥用法	厂 关键	
标准密钥用法	服务端认证	
	写 客户端认证	
	<ul><li>□ 代码签名</li><li>□ Email保护</li></ul>	
	□ 时间数 □ OCSP签名	
	□ 町回数 □ OCSP签名 □ 智能卡登录	
自定义密钥用法	□ OCSP签名 □ 智能卡登录	OID 添加自定义 <del>增</del> 级密钥用法
	□ OCSP签名 □ 智能卡登录	OID
自定义密钥用法。 Netscapel证书类型	□ OCSP签名 □ 智能卡登录	OID
	□ OCSP签名 □ 智能卡登录  ■   □   □   □   □   □   □   □   □   □	OID
	□ OCSP签名 □ 智能卡登录 ■ 対象・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	OID
	□ OCSP签名 □ 智能卡登录 □ 大健 □ SSL客户 □ SSL服务 □ SALME	OID
	□ OCSP签名 □ 智能卡量录  □ 常能卡量录  □ SSLをP □ SSL服务 □ SNIME □ 対象签名	OID 添加自定义增强密钥用法
	□ OCSP签名 □ 智能卡量录  ■ 常能卡量录  □ SSL念戸 □ SSL服券 □ SALME □ XJME □ XJME □ XJ参を名 □ SSLCA	OID
	OCSP签名 「智能卡提录 「常能卡提录 「 SSL 窓戸 「 SSL 服务 「 SALM E 「 対象変名 「 SSL CA 「 SML ECA	OID
Netscapel正书类型	OCSP签名 「智能卡提录 「常能卡提录 「SSL/客户」 「SSL/R/S 「SNLM/E 「対象を名 「SSLCA」 「SML/ECA」 「対象を名CA	
Netscapel证书类型 策略映射	□ OCSP签名 □ 智能卡登录  □ 常能卡登录  □ SSLSP □ SSL服务 □ SSLIM条 □ SMINE □ 対象签名 □ SSLCA □ SMINECA □ 対象签名CA □ 大健	□ 证书申请时必须指定值
Netscapel证书类型 策略映射 策略限制	□ OCSP签名 □ 智能卡登录 □ 智能卡登录 □ SSL态户 □ SSL离今 □ SSLM条 □ SALDAE □ 対象签名 □ SSLCA □ SMINAECA □ 対象を名CA □ 关键 □ 关键	□ 证书申请时必须指定值 □ 证书申请时必须指定值
	□ OCSP签名 □ 智能卡登录  □ 常能卡登录  □ SSL 客户 □ SSL 服务 □ SSL MA □ SMINE □ 対象签名 □ SSL CA □ SMINECA □ 対象签名CA □ 大健 □ 大健	□ 证书申请时必须指定值 □ 证书申请时必须指定值
Netscapel证书类型 策略映射 策略限制	□ OCSP签名 □ 智能卡登录  ■ 禁能・登录 □ SSL念戸 □ SSL服务 □ SSLM务 □ SSLCA □ 対象签名 □ SSLCA □ 対象を名CA □ 大健 □ 大健 □ 大健 □ 大機	□ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值
Netscape证书类型 策略映射 策略限制	□ OCSP签名 □ 智能卡登录  □ 常能卡登录 □ SSL念戸 □ SSL服务 □ SALDAE □ 対象签名 □ SSLCA □ SMINECA □ 対象を名CA □ 关键 □ 子键 □ 戸地址 □ 电子邮件地址	□ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值
Netscape证书类型 策略映射 策略限制	□ OCSP签名 □ 智能卡登录  □ 禁能卡登录 □ SSLS名戸 □ SSL服务 □ SAIDME □ 対象签名 □ SSLCA □ SMENECA □ 対象签名CA □ 关键 □ 关键 □ 戸地址 □ 电子邮件地址 □ 用戸甄別名	□ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值
Netscape证书类型 策略映射 策略映制	□ OCSP签名 □ 智能卡登录 □ 常能卡登录 □ SSLSP □ SSLBS □ SSLER S SAIDAE □ 対象签名 □ SICA □ 対象签名 □ 大健 □ 大健 □ 大健 □ 戸地址 □ 电子邮件地址 □ 用户甄別名 □ 其它名称	□ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值
Netscape证书类型 策略映射 策略映制	□ OCSP签名 □ 智能卡登录 □ SSL SP □ SSL MS □ SSL MS □ SSL MA □ SMINEC □ 对象签名 □ SSL CA □ SMINECA □ 对象签名CA □ 关键 □ 大键 □ P地址 □ 用子邮件地址 □ 用子邮件地址 □ 用子邮件地址 □ 用子邮件和址 □ 用子部外别名 □ 其它名称 □ 域名	□ 证书申请时必须指定值
Netscape证书类型 策略映射 策略限制	□ OCSP签名 □ 智能卡登录 □ 常能卡登录 □ SSLSP □ SSLBS □ SSLER S SAIDAE □ 対象签名 □ SICA □ 対象签名 □ 大健 □ 大健 □ 大健 □ 戸地址 □ 电子邮件地址 □ 用户甄別名 □ 其它名称	□ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值 □ 证书申请时必须指定值

图 25-6 证书模板定义:标准扩展项

## 2. 用户管理

用户特指证书申请者或证书所有者。证书中 Subject 与证书所有者不一定一致。用户管理基本要求如下:

① 用户分为 2 类: 个人和单位。单位可以是法人或政府机关,也可以是法人或政府机关内的某个部门。

- ② 应支持独立的用户管理功能,以方便客户分析、挖掘、跟踪等。
- ③ 每个用户可拥有多个证书。
- ④ 用户信息与证书中的信息有交叉。可以设定映射关系,避免重复录入。
- ⑤ 用户证书到期前应提供提醒机制: 短信、邮箱等。
- ⑥ 用户身份核验时,企业只需提供营业执照、税务登记证或组织机构代码证之一即可;由于企业名称变更后营业执照或税务登记证编号可能会发生编号(组织机构代码不变),因此企业用户的唯一标识应慎重考虑。

### 3. 项目管理

项目是客户(系统所有者)或同类用户(证书所有者)的统称。客户与用户关系如图 25-7 所示,如国税局为客户,网上报税系统的所有者为国税局,用户即证书所有者为报税企业。

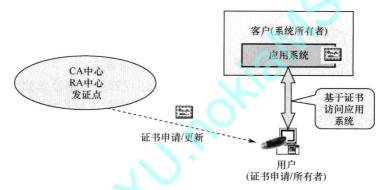


图 25-7 客户与用户关系图

项目管理基本要求如下:

- ① 项目允许多级。
- ② 项目应包括多个产品。

### 4. 产品管理

产品特指数字证书。

产品管理基本要求如下:

- ① 产品应隶属于某个项目。
- ② 产品应基于证书模板建立。
- ③ 多个产品可以基于相同的证书模板。
- ④ 应能设置某类产品所允许的介质类型,允许多个。
- ⑤ 产品应能设置待录入信息的缺省值,如 DN 项中 C/S/L/O/OU、有效期、介质类型等。
- ⑥ 产品应能设置应提交的业务资料清单(依据 CPS)。

### 5. 介质管理

介质特指用户私钥及证书载体,如 Key或 IC 卡等。

介质管理基本要求如下:

- ① 可给发证点、项目或项目中证书类型设定所允许的介质类型。
- ② 介质应具有唯一的硬件序列号,在证书申请时系统应能自动记录该序列号。
- ③ 当已有介质重复申请证书时,应自动提示。