国家环境信息与统计能力建设项目

环境身份认证技术规定

Technology regulations for environmental identity authentication

（征求意见稿）

《环境身份认证技术规定》编制组

2010 年 10 月

目　录

环境身份认证技术规定

1　适用范围

本技术规定规定了环境身份认证数字证书格式和业务管理流程及管理办法。

本技术规定不涉及任何具体的密码运算，所有密码运算均在符合国家有关法律法规的密码设备中进行。凡涉及密码相关内容，按国家有关法律法规实施。

本技术规定适用于全国各级环境保护部门的身份认证，包括电子认证服务机构、数字证书认证系统及相关产品的供应商、应用开发商的设计和开发。环境身份认证数字证书格式适用于认证机构证书、环境个人证书、环境机构证书、环境设备证书、环境服务器证书、环境应用系统证书。

2　认证证书格式

认证证书格式规范包括数字证书基本格式、个人证书格式、机构证书格式、设备证书格式。详见《国家政务外网数字证书格式规范 v7.2》。

3　认证机构（CA）命名空间

认证机构（CA）命名空间规范包括了个人数字证书主体信息、机构数字证书主体信息、设备数字证书主体信息、代码签名数字证书主体信息。详见《国家政务外网证书认证机构（CA）命名空间规范 v7.0》。

3.1　个人数字证书主体信息

表 1 个人数字证书主体信息

数据项名称	数据项描述	数据项定义及说明	采用标准
CN	用户姓名	用户姓名	例如：张三
E	电子邮件	用户邮件地址	例如：zhangsan@gov.cn
OU	组织部门	地市/厅局级组织名称	可选
O	组织名称	各个部委或是省份的名称	
C	国　　家	CN	

3.2　机构数字证书主体信息

表 2 机构数字证书主体信息

数据项名称	数据项描述	数据项定义及说明	采用标准
CN	机构名称	使用中文	例如：XX市环境信息中心
E	机构电子邮件	邮件地址	例如：xinxizx@gov.cn
OU	组织部门	地市/厅局级组织名称	可选
O	组织名称	各个部委或是省份的名称	
C	国　　家	CN	

3.3 设备数字证书主体信息

表 3 设备数字证书主体信息

数据项名称	数据项描述	数据项定义及说明	采用标准
CN	名称	域名或IP	例如：www.cei.gov.cn
OU	组织部门	地市/厅局级组织名称	可选
O	组织名称	各个部委或是省份的名称	
C	国　　家	CN	

3.4 代码签名数字证书主体信息

表 4 代码签名数字证书主体信息

数据项名称	数据项描述	数据项定义及说明	采用标准
CN	开发机构名称		例如：国家信息中心
OU	组织部门	地市/厅局级组织名称	可选
O	组织名称	各个部委或是省份的名称	
C	国　　家	CN	

4 证书认证机构（CA）系统接口

环境身份认证技术规定系统接口包括数字证书应用接口体系结构、数字证书应用接口组成和功能说明和数字证书应用接口函数定义。详见《国家政务外网证书认证机构（CA）系统接口规范 v7.0》。

5 证书注册机构（RA）建设

5.1 环境建设

5.1.1 机构名称

按照国家政务外网注册服务点（RA）建设要求下发的文件为依据，到当地密码管理部门申请成为“**省环境身份电子认证服务中心”。

5.1.2 办公场地

需要办公用品包括：个人计算机（至少3台，用于制证及RA系统管理）、标签打印机、扫描仪、复印机、办公桌、办公椅、铁皮柜（用于存放客户资料，存储介质等）、保密柜（存放保密物品，如：未被用户领走的存有私钥的介质）。

根据以上办公物品存放面积、人员工位大小及受理接待区，建议至少40平方米。

5.1.3 机房

在标准机房内放置一至两个机柜，用于安装RA服务器、目录服务、密码机和相关安全防护设备。

5.1.4 人员配置

需配置至少2位工作人员，职责包括用户接待、资料录入、资料审核、制作证书、原材料出入库、证书出入库、对证书、原材料进行汇总统计管理、产品的派送、原材料采购、制证档案资料管理等。要求人员具备中专以上学历，熟悉办公软件的使用，录入速度70字/分

钟以上。其中，资料录入与资料审核需两人分别办理，其他可兼职进行。随着业务量的增多，再增补人员。

5.1.5 人员培训

1、RA 运维培训，由环境保护部统一组织安排。

2、RA 技术培训，由 RA 产品提供商安排。

5.1.6 环境保护部产品列表

表 5 环境保护部产品列表

类别	具体模块	数量	备注
软件	注册审核系统	1	
	统一用户管理系统	1	
	目录服务系统	3	
	操作系统	4	Windows 2003 Server 或以上版本
	数据库系统	1	
硬件	身份认证网关	1	
	主机服务器	4	PC Server 服务器
	加密机	1	
	USB KEY		
	磁带机	1	
	管理终端	5	CPU2.0GHz 硬盘：250G 内存：2G 光驱：DVD-RW （或高于以上配置）

5.2 节点（RA）

5.2.1 系统功能

a) 符合《国家电子政务外网 CA 接口规范》，可以直接接入国家电子政务外网运行 CA，采用国家电子政务外网运行 CA 提供的服务。

b) 使用国家密码管理局《证书认证系统密码及其相关安全技术规范》中的安全通信标准与国家电子政务外网运行 CA 进行安全通信。

c) 提供基本的证书信息管理服务，包括：

1) 注册
2) 签发审核
3) 证书签发
4) 更新申请
5) 更新审核
6) 证书更新
7) 废除申请
8) 废除审核
9) 证书废除
10) 重发申请
11) 重发审核
12) 证书重发

13) 信息注销

d) 提供基本的证书辅助管理功能包括查询/统计/归档等。

e) 对外提供服务接口，供第三方方便地进行应用开发。

5.2.2 系统结构

节点RA结构要求符合国家密码管理局的相关规定，系统结构设计如下所示：

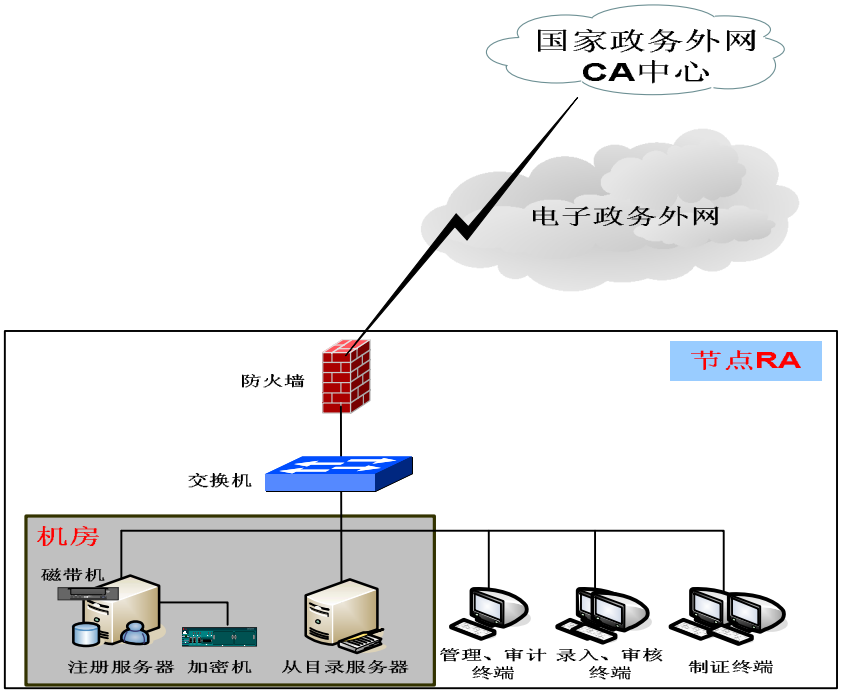

图 1：节点 RA 系统结构设计图

由上图可见，节点RA需要通过防火墙与国家电子政务外网CA中心相连，防火墙要求只开放必要的端口。RA系统中注册服务需要通过加密机来保存RA系统的密钥，并用加密机实现与政务外网运行CA的安全通讯。加密机要求采用符合国家密码管理局要求的产品。从目录服务系统需要与政务外网的主目录服务系统相联，要求能够实现与政务外网目录服务数据同步、复制、查询。

为保证数据的安全，采用磁带机等存储方式对RA系统的数据进行备份处理。RA中心至少部署一台用于系统管理和审计的终端，一台录入终端、一台审核终端和两台制证终端。系统要采取防病毒等安全保障措施，具体可根据实际情况设计选用相应的产品及措施。

节点 RA 接入国家电子政务外网运行 CA 时，需要遵循国家电子政务外网发布的 CA 系统接口规范。详见《国家电子政务外网 CA 接口协议》。

5.2.3 目录服务系统

目录服务系统的规范，需要遵循国家电子政务外网发布的注册服务点 RA 建设规范。详见《国家电子政务外网注册点 RA 建设指南 V8.1》

6 证书注册机构（RA）业务流程及管理

6.1 数字证书的签发

6.1.1 证书签发中 RA 和 CA 的行为

RA 业务管理员使用证书登录到 RA 系统的业务终端，查询并审核系统的申请记录。审核通过的信息将发送到证书认证机构的 CA 系统，CA 系统签发证书并返回给 RA 系统供终端实体下载。政务数字证书注册机构（RA）和受理点建设参见附录 D。

6.1.2 密钥对的安全技术控制

6.1.2.1 CA 公钥的发送

证书认证机构的根 CA 公钥，通过如下方式传输给依赖方：

a) 依赖方访问证书认证机构的网站下载 CA 根证书；

b) 证书认证机构到依赖方业务系统现场将 CA 根证书安装到业务系统中；

c) 证书认证机构通过签名电子邮件将 CA 根证书传输给依赖方；

d) 证书认证机构将 CA 根证书绑定在分发给依赖方的软件中。

6.1.2.2 终端实体密钥对的产生和发送

对于个人证书、机构证书和代码签名证书，终端实体的签名密钥应使用 USB Key 产生；对于设备证书、服务器证书和应用系统证书，终端实体可利用设备或服务器自带程序软件提供的密钥生成功能产生密钥对，也可采用专门硬件模块产生密钥对。

终端实体的加密密钥对应由国家密码管理部门许可的、证书认证机构签发系统支持的加密机设备产生，由 KMC 管理。

终端实体的加密私钥只保存在 KMC 和终端实体介质。在加密私钥从 KMC 到终端实体的传递过程中应采用国家密码管理部门许可的算法加密。

终端实体的签名证书公钥通过安全通道经 RA 传递到 CA。

终端实体的加密证书公钥，由 KMC 通过安全通道传递到 CA。

终端实体的公钥在从 RA 到 CA 以及从 KMC 到 CA 传递过程中，应采用国际密码管理部门许可的通讯协议及密码算法。

6.1.2.3 密钥对使用期限

密钥对的使用期限和其对应的终端实体证书的有效期一致。

6.1.3 数字证书发布

证书认证机构在证书签发完成后，将数字证书发布到服务器中供终端实体和依赖方查询和下载。

6.2 数字证书的使用

6.2.1 数字证书使用范围

在全国环保电子政务中涉及到身份认证、数据传输、安全邮件、数据交换活动，通过本规范的应用接口与相关技术协议支持数字证书。

在全国环保电子政务涉及到各级环境保护部门门户的身份认证和登录应支持数字证书。

在全国环保电子政务涉及到跨省、市、县的应用系统应使用数字证书。

在全国环保电子政务涉及到部门内部系统宜使用数字证书。

6.2.2 依赖方的证书使用

依赖方接收到经数字签名的信息后：

a) 获得数字签名对应的证书及信任链；

b) 确认该签名对应的证书是依赖方信任的证书；

c) 检查证书的有效期，确认该证书在有效期内；

d) 查询证书状态，确认该证书没有被注销；

e) 证书的用途适用于对应的功能；

f) 使用证书上的公钥验证签名。

以上任一环节失败，依赖方拒绝接受签名信息。

依赖方需发送加密信息给接受方时，应先获取接受方的加密证书，并使用证书公钥对信息加密，将加密证书连同加密信息一起发送给接受方。

6.3 数字证书的维护

证书认证机构实现对政务数字证书的更新、变更、吊销与挂起。

6.4 数字证书的载体

对于设备证书、服务器证书和应用系统证书，载体为设备硬盘或加密硬件设备。

对于个人证书、机构证书和代码签名证书，载体为 USB Key，功能包括：

a）提供数据、私钥和算法安全存贮功能，私钥不可复制，对外不可读，具备多密钥存储功能；

b）采用国家密码管理部门批准的硬件物理噪音源生成随机数；

c）支持 PKCS#11、X.509 V3 证书存储及 Microsoft CrptoAPI 应用接口标准；

d）USB Key 的设备驱动程序附有主流操作系统的硬件设备认证签名；

e）提供 PIN 口令保护机制；

f）密钥在 USB Key 硬件内部生成；

g）具有 LED 用于电源指示和通讯指示。

6.5 数字证书实体的查询

证书认证机构通过以下方式提供数字证书的实体查询：

a) 在其网站提供证书实体查询及公钥证书下载服务；

b) 发布 CRL 提供证书状态查询服务；

根据依赖方应用系统实时性和并发量需求协商提供在线证书查询（OCSP）服务或目录服务器（LDAP）查询服务。

6.6 数字证书更新请求确认

6.6.1 更新申请情况

a）证书到期；

b）证书补发；

c）证书DN或EMAIL更改；

d）密钥更新。

出现以上情况时证书用户可以到环境保护部授权的发证机构申请更新证书。

6.6.2 更新操作

证书用户申请更新证书时，填写证书更新表（一式三份），按照初始身份验证步骤提交相关资料并由环境保护部授权的发证机构审核。

6.6.3 更新申请的确认

环境保护部授权的发证机构的审核人员合理、审慎地核对申请资料的原件与复印件，根据审核人员的管理规定对申请者的资料的真实性进行表面审查，并进行批准或拒绝的操作。

6.7 数字证书废止请求确认

6.7.1 证书废止情况

a）密钥泄漏；

b）证书有效期内用户终止使用证书；

c）其它。

证书废止包括证书废除、证书挂起。

6.7.2 证书废止操作

证书用户申请废止证书时，填写证书废止表（一式三份），按照初始身份验证步

骤提交相关资料并由环境保护部授权的发证机构审核。

6.7.3 证书废止申请的确认

环境保护部授权的发证机构的审核人员合理、审慎地核对申请资料的原件与复印件，根据审核人员的管理规定对申请者的资料的真实性进行表面审查，并进行批准或拒绝的操作。

6.8 数字证书恢复请求确认

6.8.1 证书恢复情况

只能恢复被挂起的证书。

6.8.2 证书恢复操作

证书用户申请恢复证书时，填写证书恢复表（一式三份），按照初始身份验证步骤提交相关资料并由环境保护部授权的发证机构审核。

6.8.3 恢复申请确认

由环境保护部授权的发证机构的审核人员合理、审慎地核对申请资料的原件与复印件，根据审核人员的管理规定对申请者的资料的真实性进行表面审查，并进行批准或拒绝的操作。

7 证书注册机构（RA）管理与操作安全控制

7.1 物理安全控制

7.1.1 机房安全

所有机房的建设和管理严格按照环境保护部对机房的规定要求。机房内部一律禁止参观，只有经过授权的人员才能进入授权的部门和工作地点。在进入机房时，必须经过身份识别。

监控记录,监控记录文件包括对机房通道上的所有踪迹的记录。环保部门的员工经授权后，两人以上才能进入机房。对于要进入机房的来访者，要经环境保护部运营安全管理小组批准后，指定并授权一位环保部门的员工陪同。

受理点网络系统保护,所有环境保护部RA受理点的网络系统也必须受到保护,确保只有经授权的员工才能进入受理点的系统。环境保护部的管理员负责设置和检查受理点管理员的权限。

7.1.2 电源和空调

环境保护部身份认证系统采用双电源供电，在单路电源中断时，可以维持系统正常运转。同时，使用一个不间断电源（UPS），避免电源波动。

环境保护部身份认证系统使用中央空调和冷却设备。

环境保护部身份认证系统对电源，空调等要求，按照电信设施管理的规定严格要求，并且每年对是否符合要求进行检查。

7.1.3 防火

通过与专业防火部门协调，实施消防灭火等应急响应措施，避免火灾的威胁，充分保障系统安全。

7.1.4 存储介质保护

存储介质必须得到安全可靠的保护，避免诸如温度、湿度和磁力等环境变化可能产生的危害和破坏。

7.1.5 过期数据处理

当电子认证服务机构保存的相关数据已不再需要或存档的期限已满时，由环境保护部将完全销毁这些数据。

所有处理行为将记录在案，以供审查的需要，销毁行为遵守我国的法律。

7.2 流程安全控制

7.2.1 职位分配

环境身份认证明确执行认证系统的关键职能职位，他们包括：

a) 运营安全管理小组

享有以下权限：

1）提出安全管理策略方面的建议；

2）负责安全措施的制定和定期进行安全审计；

3）能够及时地对系统的安全问题做出响应，减少因处理不及时所造成的损失；

4）开发并维护环境身份认证业务规则；

5）确保环境身份认证业务规则的政策能够通过技术解决方式得到实施；

6）保障环境身份认证系统的运营同电子认证业务规则保持一致；

b) 系统管理员

享有以下权限：

1）建立和变更环境身份认证安全策略；

2）增加和减免其他安全官员，管理员，及用户；

3）对于敏感操作的授权，诸如增加和减免安全官员及管理员；

4）管理交叉认证，发布环境身份认证交叉认证协议，更新及注销交叉认证；处理审计日志；

5）管理CRL、证书模板的制定。

c) 信息录入员

1）负责用户证书申请信息的录入；

2）协助客户办理数字证书申请、作废、更新等手续。

d) 审核员

1）负责数字证书的审批受理；

2）如实向上级机构传送证书申请者的信息；

3）协助客户办理数字证书申请、作废、更新等手续。

e) 审计员

1）负责RA数字证书的统计、审计；

2）负责RA日志的备份、恢复。

f) 制证员

1）证书的制作、发放；

2）协助客户办理数字证书申请、作废、更新等手续。

g) 其他管理员

包含：

1）网络管理员

2）数据库管理员

3）加密机管理员

4）目录服务管理员

5）证书发布系统管理员

7.2.2 人员数量要求

环境身份认证系统确保单个人不能接触、导出、恢复、更新、废止环境身份认证的CA系统存储的根证书对应的私有密钥。

至少两个人才能使用一项对参加操作人员保密的密钥分割和合成技术，进行CA系统中密钥恢复的操作。

对与运行和操作相关的职能有明确的分工，贯彻互相牵制的安全机制。

7.3 日志审计

7.3.1 记录事件种类

环境身份认证的RA运行系统，记录所有与系统相关的事件，以备审查。这些记录，无论是手写、书面或电子文档形式，都包含事件日期、事件的内容、事件的发生时间段、事件相关的实体等。

7.3.2 审查的频率

每周对记录进行审查，对审查记录行为备案。

7.3.3 审查记录的保存期限

在数据库保存审查记录至少两个月，离线存档至少七年。

7.3.4 审查记录的保护

环境身份认证执行严格的通道管理，确保只有环境保护部授权的人员才能接近这些审查记录。这些记录处于严格的保护状态，并且有异地备份，严格禁止访问、阅读、修改和删除等操作。

7.3.5 审查记录备案步骤

环境身份认证保证所有的审查记录和审查总结都按照相关备份标准和程序进行。根据记录的性质和要求，采用在线和离线的各种备份工具，有实时、每天、每周、每月和每年等各种形式的备份。

7.4 归档策略

7.4.1 记录的事件类型

环境身份认证会对RA的数据库定期存档，间隔时间由环境保护部自行决定，存档的内容包括环境身份认证发行的证书和CRL、审查数据记录、证书申请审批资料等。

7.4.2 存档的保留期限

环境身份认证中的存档期限一般规定为七年。

7.4.3 档案的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能接近它们。保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力等的破坏。

7.4.4 存档备份

所有存档文件的数据库除了保存在环境保护部的主要存储库，还将在异地保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有授权的工作人员才能在监督的情况下，对档案进行读取操作。环境身份认证在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

7.5 密钥转换

7.5.1 密钥转换定义

在这里密钥转换是指当环境身份认证根证书到期而需要更换根密钥对时所采取的措施。环境身份认证根密钥对由加密机产生。证书到期更换密钥时将签发3张证书。

a）使用旧的私有密钥对新的公钥及信息签名生成证书；

b）使用新的私有密钥对旧的公钥及信息签名生成证书；

c）使用新的私有密钥对新的公钥及信息签名生成证书。

通过以上3张证书达到密钥更换的目的，使新旧证书之间互相认证、信任。

7.5.2 根证书有效期

环境身份认证根证书有效期为10年。在环境身份认证证书到期之前，环境保护部将对根私有密钥进行更换。密钥转换程序在旧密钥对向新密钥对的转换起着过渡的作用。环境身份认证密钥转换采用以下方式：

a）环境身份认证将在证书到期前的60天内停止颁发新的证书；

b）旧的环境身份认证证书到期后，环境保护部将用新的CA密钥对签发证书。

7.5.3 CRL

新的环境身份认证将继续使用旧的 CA 根私有密钥签发的 CRL，直到由旧的 CA 根私有密钥签发的证书到期为止。

8 证书受理点（LRA）建设

8.1 身份认证网关

a) 用户身份认证：提供对外身份认证服务，同时支持基于 PKI/CA 数字证书和用户名/口令的身份认证方式，可以单独使用也可组合使用。

支持集中认证，作为认证的发起点，支持联合多种其他类型的认证服务，为用户做统一认证。

b）单点登录：支持多个应用系统之间的单点登录，即一次登录，多次使用。

c）应用级控制：管理员可以通过策略配置，授权用户对应用系统的访问。

d) 状态监控：系统支持通过图形界面实时对当前运行状态进行监控，便于系统的维护和问题定位。

e）日志审计：系统可以按照系统日志、业务日志两大类日志对用户、管理员使用系统过程进行完整审计。审计管理员可以对指定范围内的日志进行查询系统使用情况，为管理员和决策者提供最有效的数据支持。

f）分权管理：系统内设系统管理员、安全管理员、审计管理员。系统管理员负责对软件环境日常运行的管理和维护，以及对系统的备份和恢复操作系统管理员负责执行系统的数据库备份策略和软件系统备份策略；安全管理员负责网关业务配置、应用管理、授权管理等管理操作；审计管理员负责对系统日志查询、归档等管理操作。

g）备份恢复：系统支持备份恢复功能，可以快速恢复系统的正常工作。当系统运行环境遭到破坏时，可以通过备份数据，快速的进行恢复，将损失程度降到最低。备份数据包括系统配置数据及系统业务数据。配置策略包括即时备份和手动备份两种策略。即时备份指当运行环境发生改变的情况下（如修改了系统的相关配置），进行即时的系统备份。手动备份策略为管理员通过管理平台备份功能把当前运行良好的环境进行备份，可以将备份文件下载到本地；可以通过配置上传恢复功能将相同当前运行环境恢复到某一备份配置。

备份与恢复功能主要包括系统的出厂设置、系统的备份、系统的恢复、系统升级等功能。

h）系统配置管理：系统支持串口管理、WEB 管理两种方式。串口管理采用命令行管理模式，管理员通过串口线登录到网关系统，通过命令行交互界面执行相关的命令。WEB 管理是指管理员通过浏览器登录到网关系统，通过管理界面进行相关配置工作。

8.2 目录服务器系统（LDAP）

目录服务系统主要负责发布数字证书和证书注销黑名单数据，为应用进行证书校验提供依据。

环境保护部目录服务系统和国家政务外网目录服务系统之间形成主从的关系，国家政务外网目录服务系统实时的把数据同步到环保部目录服务系统中。环保部应用系统由本地的目录服务系统获取相应的数字证书和黑名单数据，可以有效的提升应用系统的访问速度和稳定

性。

在目录复制策略方面，环境保护部目录服务系统选择部分复制方式实现目录服务部署，即仅复制政务外网运行 CA 主目录服务器中的环境保护部相关信息，在保证了本地用户访问本地目录效率的同时，又避免了过多无用信息复制可能造成的网络拥塞。

环境保护部全目录服务器与各下属省厅目录服务系统之间的复制策略是可制订的，用户可以采用实时、定时复制两种策略。实时复制的优点是可以保证主服务器的数据变化及时更新到从目录服务器，缺点是对网络状况要求较高，定时复制则与实时复制相反，鉴于用户的网络环境原因建议使用定时复制，在网络比较顺畅的时间进行复制，定制可以按照星期、日期进行设置。

a）按照星期进行设置的内容如下：

1）选择星期(从星期一到星期日至少要选中一个)；

2）选择时刻(时刻为 小时：分)，时刻精确到分。

b）按照日进行设置的内容如下：

1）选择日(可选择多天）；

2）选择时刻(时刻为 小时：分)，时刻精确到分。

当定时计划设置完成后，如果系统到了所设置的定时时间，复制进程可以自启动，复制进程处理完更改日志后自动停止。

8.3 加密机

RA 系统中选择 56 所的 SJY42 主机密码服务器作为这个体系的加密设备,提供基础的密码服务。

SJY42 主机加密服务器是 PKI 通用网络安全服务平台的高端核心设备，已通过国家密码管理委员会办公室技术鉴定，位于安全平台的最底层——硬件加密层，其主要功能是为上层应用系统提供所需的密码运算服务以及执行系统中已制定的安全策略。它主要有如下特点：

a) 合理清晰的模块化设计，超前新颖的设计思想；
b) 对连接主机的高兼容性和高扩展性；
c) 性能稳定可靠，容错性能高，完备的热备和冷备功能；
d) 安全存储密钥：通过严格的安全机制保存密钥，即使加密机被盗、丢失，其中的密钥也不能被非法读出；
e) 安全存储加密机核心程序：加密机使用带有逻辑加密功能的芯片对核心程序进行存储，防止非法读出；
f) 多级权限管理：加密机内可以设置管理员和操作员，分别赋予不同的权限，实现权限分割，进一步保证加密机内数据和程序的安全；
g) 口令安全性：对管理员和操作员身份，通过 IC 口令卡进行识别；
h) 密钥管理安全性：加密机内存储的密钥一经生成，在任何情况下不允许以明文形式输出卡外；
i) 加密服务器主机与客户端主机之间采用高速稳定的 TCP/IP 网络通信，并且在网络传输过程中的数据均为经过加密的密文数据，保证了其传输的安全性；
j) 公钥运算能力大幅提高：加密机内加密卡设备使用多颗专用公钥芯片进行 RSA 公钥算法运算，使得公钥处理速度提高了几十倍；
k) 加密机使用国家密码管理办公室专门研制的支持 SSF33 密码算法专用芯片。SSF33 密码算法是国家密码管理办公室根据商密发展需要，作为 IC 卡和 CA 应用标准算法而研制的；
l) 方便有效的控制方式和友好、直观的操作界面；
m) 完备的监控模块，并且支持双机热备份和负载均衡的工作方式；

n) 高速的网络运算连接服务；
o) 系统本身的高扩展性，安全方便的升级方式。
p) 提供国家规定密码算法保护机制；
q) 128 位对称算法加解密速度不低于 60Mbps；
r) 1024 位密钥对生成速度大于 3 对/秒；
s) 1024 位签名速度大于 2000 次/秒；
t) 1024 位验证速度大于 10000 次/秒；
u) 支持 Windows2000/XP/2003、UNIX、Linux 等操作系统；
v) 提供标准 API，支持 PKCS#11 接口、X.509 证书接口、CSP 接口和国际主流安全协议；
w) 支持多进程和多线程操作；
x) 具备多级权限管理功能；
y) 具备密码卡扩展能力；
平均无故障时间高于 3000 小时；

8.4 USB KEY

采用 USBkey（密码钥匙），主要用来存储证书/密钥和完成相关密码运算。它使用方便安全性高，已经在整个领域得到了充分的使用。

8.4.1 产品特性

a) 内置 CPU 智能芯片，具有智能 IC 卡操作系统的所有功能。
b) 支持国家安全密码管理委员会批准的分组密码算法、同时兼容 DES/3DES 密码算法，实现加密解密功能。
c) 支持 RSA1024bit 的公私钥算法及其密钥对生成，可实现签名/验证、身份识别功能。
d) 支持 SHA-1、MD5 的摘要算法。
e) 支持国产 SSF33 算法。
f) 支持 SCB2 密码算法；
g) 支持 Windows xp 、Vista 、Windows 7 操作系统的 32 位和 64 位版本
h) 内置硬件随机数发生器。
i) 具有一个 LED，用于电源指示和通讯指示。
j) 驱动程序通过微软 WHQL 认证。

8.4.2 技术指标

a) USB 通讯接口，速率 1.5Mbps。
b) 用户存储空间为至少为 32K，可用于安全存储个人信息、密钥、数字证书。
c) X509 数字证书存储。
d) 电源 5±10%V，由 USB 接口直接供给。
e) 环境温度：0℃~70℃。
f) 相对湿度：30%~95%。
g) 抗静电干扰：4KV。
h) IC 芯片可使用 10 万次以上，USBKEY 插拔次数一万次以上。

8.4.3 性能指标

a) 数据读

X．509V3 的证书大小约为 2K 字节，因此对智能钥匙读写速度测试数据量设定为 2K 字节。测试时连续进行 100 次读 2K 数据的操作，操作所需时间的平均值为 668 毫秒。

b) 数据写

测试时连续进行 100 次写 2K 数据的操作，操作所需时间的平均值为 1843 毫秒。

c） 产生 1024 位密钥对

为了保证私钥的安全，密钥由智能钥匙产生。与私钥有关的运算均在智能钥内完成，私钥永远无法读出。测试时连续进行 100 次产生 1024 位密钥对的操作。所统计的是产生密钥对和回传公钥操作所占有的时间。操作所需时间的平均值为 8900 毫秒。

d） 1024 位签名

在输入 HASH 结果后，USBKEY 可以用其 1024 位的私钥进行签名。经统计操作所需时间的平均值为 283 毫秒。

e） 标准操作

所谓标准操作包括建立智能钥匙与计算机主机之间的连接，智能钥匙的复位上电，验证个人密钥，读 2k 字节数据，智能钥匙下电和释放 USB 接口等操作。在两组操作有 2 秒的间隔（不计时）以保证测试与实际运用情况更接近。测试时进行 100 组操作，操作用时的平均值为 231 毫秒。

8.5 推荐配置列表

8.5.1 省级单位产品配置列表

表 6 省级单位产品配置列表

类别	具体模块	数量	备注
软件	统一用户管理系统（UMS）	1 套	
	目录服务系统	2 套	
	受理点管理系统	1 套	
	操作系统	4 套	Windows 2003 Server 或以上版本
硬件	身份认证网关	1 台	
	主机服务器	4 台	PC Server 服务器
	USB KEY		
	管理终端	5	CPU2.0GHz 硬盘：250G 内存：2G 光驱：DVD-RW （或高于以上配置）

9 证书受理点（LRA）管理

9.1 信息录入员

a） 负责用户证书申请信息的录入；

b） 协助客户办理数字证书申请、作废、更新等手续。

9.2 信息审核员

a） 负责数字证书的审批受理；

b） 如实向上级机构传送证书申请者的信息；

c） 协助客户办理数字证书申请、作废、更新等手续。

9.3 制证员

a）证书的制作、发放；

b）协助客户办理数字证书申请、作废、更新等手续。

9.4 管理员

a）负责系统日志、业务日志的审计工作；

b）负责管理身份认证网关、目录服务器系统、加密机、系统数据库等工作。

附 录 A

（规范性附录）

证书存贮介质技术要求

A.1 功能要求

a) 提供数据、私钥和算法安全存贮功能，用户私钥不可复制，对外不可读、且具备多密钥存储功能；
b) 采用国家密码管理局批准的硬件物理噪音源生成真正随机数；
c) 支持 USB 接口、PKCS＃11、Microsoft CrptoAPI、 X.509 v3 证书存储等标准；
d) USB Key 的设备驱动程序应使用微软硬件设备认证签名；
e) 支持 Windows 98/ME/2000/XP/2003 操作系统；
f) 提供 PIN 口令保护机制；
g) 支持热拔功能；
h) 支持使用 USB KEY 登录 Windows 操作系统；

A.2 密码算法要求

a） 支持 SSF33 专用对称密码算法；
b） 支持 SCB2 密码算法；
c） 对称密码算法密钥长度不低于 128 位，公开密钥算法密钥长度不低于 1024 位；
d） 公开密钥对在 USB KEY 硬件内部实时生成。

A.3 性能要求

a） 工作电流 ： <50mA
b） 待机电流 ： <300uA
c） 数据保存 ： 10 年以上
d） 读取速度 ： 不低于 1000bit/S
e） 写入速度 ： 不低于 900bit/S
f） 容量：大于等于 32Ks

附 录 B

（资料性附录）

软硬件设备参考

RA系统可利用外网网络设备，所以配置方案未包含网络设备和网络安全防护设备。RA系统的安全防护，至少包括防火墙、防病毒等安全功能。

为证书应用推广方便，RA系统可配置安全认证网关，用于快速部署身份认证系统。

B.1 推荐配置一：小型RA系统及费用估算

功能

证书容量 2 万张，日发证量最大 300 张。

硬件设备

服务器（1 台）3 万

安装 RA 管理系统及数据库。要求使用 RAID5 存储，内置磁带机。

加密机（1 台）8 万

用于安全通信

终端（3 台）1.8 万

负责制证及管理 RA 系统

软件

RA 管理系统 20 万

目录服务系统 10 万

小型数据库 6 万

共计：48.8 万

B.2 推荐配置二：中型RA系统及费用估算

功能

证书容量 5 万张，日发证量最大 800 张。

硬件设备

应用服务器（1 台）3 万

安装 RA 管理系统。要求使用 RAID 5 存储。

数据库服务器（1 台）3 万

安装数据库系统。要求使用 RAID 5 存储，内置磁带机。

目录服务器（1 台）3 万

安装目录服务系统。要求使用 RAID 5 存储。

加密机（1 台）8 万

用于安全通信

管理终端（1 台）0.6 万

负责管理 RA 系统

制证终端（4 台）2.4 万

负责制证

软件

RA 管理系统 20 万

中、小型数据库 6 万

目录服务系统 10 万

共计：56万

B.3 推荐办公设备

用于办理证书时，材料归档。
扫描仪（1 台）
复印机（1 台）
黑白激光打印机（1 台）
配套办公桌椅
铁皮柜

B.4 通过测试的RA产品

RA产品必须经过国家政务外网工程办公室测试通过，证明可以与国家政务外网运行CA联通才可使用。目前上海格尔软件股份有限公司和吉大正元信息技术股份有限公司的RA软件系统已经过测试，成功联接政务外网运行CA。如有其它厂商的RA产品通过测试，国家政务外网工程办公室会及时通知各单位。

附 录 C

（资料性附录）

安全认证网关功能

安全认证网关主要实现证书和业务系统之间的方便、快捷整合，为业务系统提供身份认证、数据传输加密的功能。安全认证网关可以和国家电子政务外网从目录服务系统或是本地的从目录服务系统之间连接，获取证书黑名单信息（CRL），实现证书有效性的验证。安全认证网关的功能要求如下：

a) 能够支持国家电子政务外网 CA 发放的证书；
b) 有和国家电子政务外网 CA 签发的证书相结合的成功案例；
c) 可以独自完成基于证书的身份认证；
d) 提供支持多证书链功能，可同时支持多个证书颁发机构颁发的证书；
e) 提供双向身份验证功能；
f) 支持 B/S、C/S 等多种类型应用接入，且无需任何改动便可直接接入网关；
g) 支持 128 位高强度数据传输加密；
h) 提供浏览、下载等日志管理功能，且可与第三方审计系统进行关联；
i) 提供数据备份和恢复功能；
j) 对外提供服务接口，供第三方方便地进行应用开发；
k) 系统性能：最大并发用户数：500 个

附 录 D

（资料性附录）

数字证书注册机构和受理点建设样例

D.1 注册机构和受理点功能

数字证书注册机构作为证书认证机构授权委托的下属机构，负责证书用户信息的审核、整理汇总、统计分析，与上级 CA 进行数据交换，管理和服务下层注册分支机构和下层受理点。每个注册机构可以按照行政地域分成多个受理点，可以直接对终端实体提供服务。政务数字证书注册机构有责任妥善保存终端实体的数据。

数字证书受理点负责审核受理证书申请实体的信息，包括申请实体的名称、可以表明身份的号码和联系方法（通信地址、电子邮件、电话）等。受理点根据这些信息为申请实体提供证书，或根据申请实体的要求，提供申请实体自行申请的技术支持。

D.2 注册机构和受理点在PKI体系中的位置

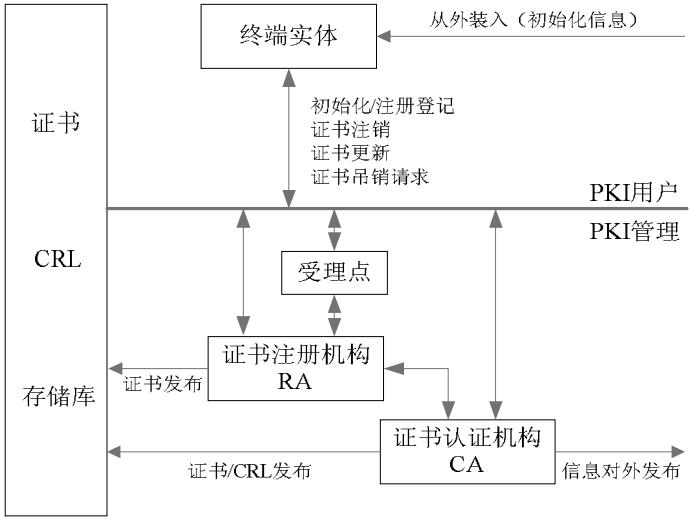

图 D.1 PKI 实体

D.3 证书注册机构逻辑结构

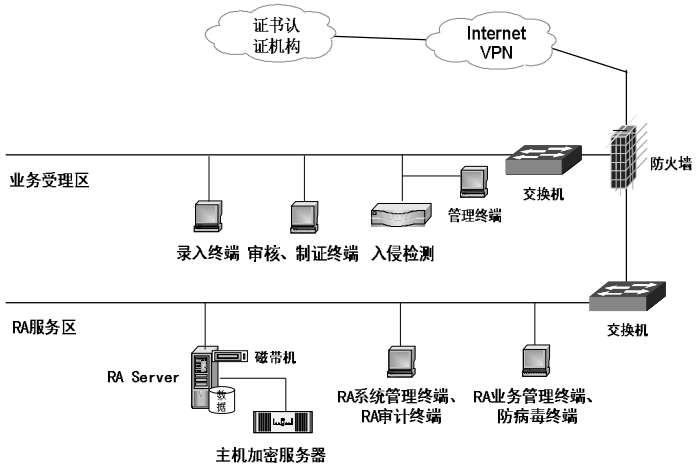

图 D.2　证书注册机构逻辑结构图

D.4 受理点逻辑结构

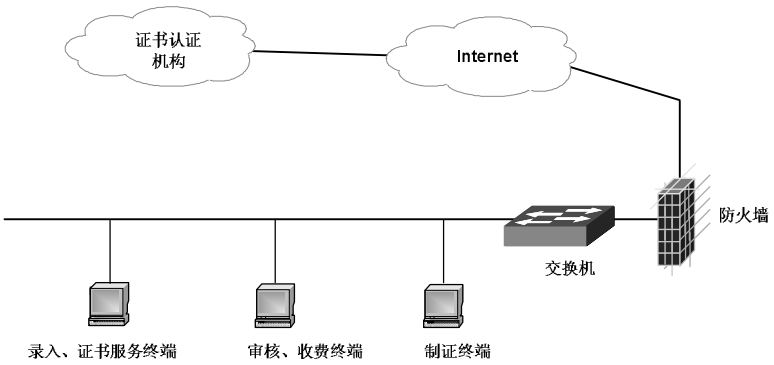

图 D.3　受理点逻辑结构图

参考文献

[1] DB 42/T 362－2006 电子政务术语
[2] GB/T 2260 中华人民共和国行政区划代码
[3] GB/T 20518-2006《信息安全技术 公钥基础设施数字证书格式》
[4] HJ/T 416 环境信息术语
[5] YD/T 1322.3-2004 电子商务技术要求 第三部分：证书及认证系统
[6] 《中华人民共和国电子签名法》
[7] 《电子认证服务管理办法》
[8] 《国家政务外网注册服务点（RA）建设指南v8.1》
[9] 《国家政务外网证书认证机构（CA）命名空间规范v7.0》
[10] 《国家政务外网证书认证机构（CA）系统接口规范v7.0》
[11] 中华人民共和国信息产业部颁布的《电子认证业务规则规范（试行）完全版》