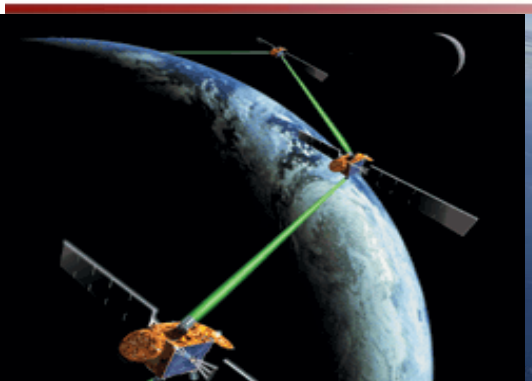
普通高等教育“十一五”国家级规划教材
教育部2011年精品教材

网络安全—技术与实践（第2版）

刘建伟 王育民 编著

清华大学出版社




课件制作人声明

- 本课件总共有17个文件，版权属于刘建伟所有，仅供选用此教材的教师和学生参考。
- 本课件严禁其他人员自行出版销售，或未经作者允许用作其他社会上的培训课程。
- 对于课件中出现的缺点和错误，欢迎读者提出宝贵意见，以便及时修订。

课件制作人：刘建伟

2016年11月01日

第9章 数字证书与公钥基础设施

一 PKI的基本概念

二 数字证书

三 PKI体系结构—PKIX模型

四 PKI实例

五 授权管理设施—PMI

第9章 数字证书与公钥基础设施

一 PKI的基本概念

二 数字证书

三 PKI体系结构—PKIX模型

四 PKI实例

五 授权管理设施—PMI

9.1 PKI的基本概念

PKI：公钥基础设施 Public Key Infrastructure

就是一种用公钥密码理论和技术实施和提供安全服务的、具有普适性的安全基础设施。

PKI的目的

解决网上身份认证、电子信息的完整性和不可抵赖性等安全问题，为网络应用提供可靠的安全服务。

PKI的任务

在电子商务和电子政务中，它可以为网络用户提供可信的数字身份认证。

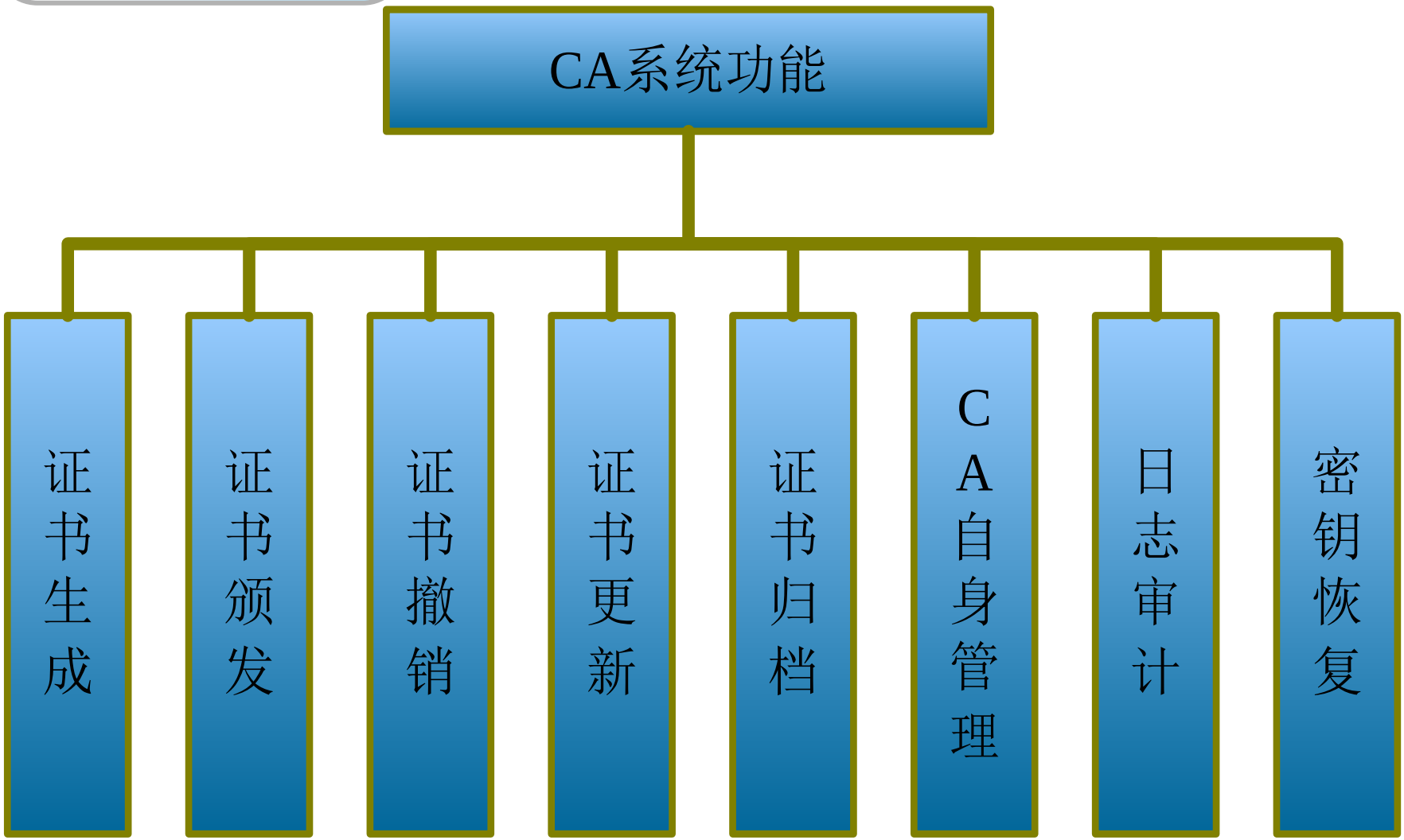
9.1 PKI的基本概念

PKI的组成

1. 证书机构CA
2. 注册机构RA
3. 证书发布库
4. 密钥备份与恢复
5. 证书撤销
6. PKI应用接口

9.1 PKI的基本概念

证书机构CA



9.1 PKI的基本概念

证书机构CA的功能

- 负责发放和管理数字证书
- 提供网络身份认证、负责证书签发及证书的管理
  - 跟踪证书状态
  - 在证书需要撤销时发布证书撤销通知
- 维护证书档案和证书相关的审计

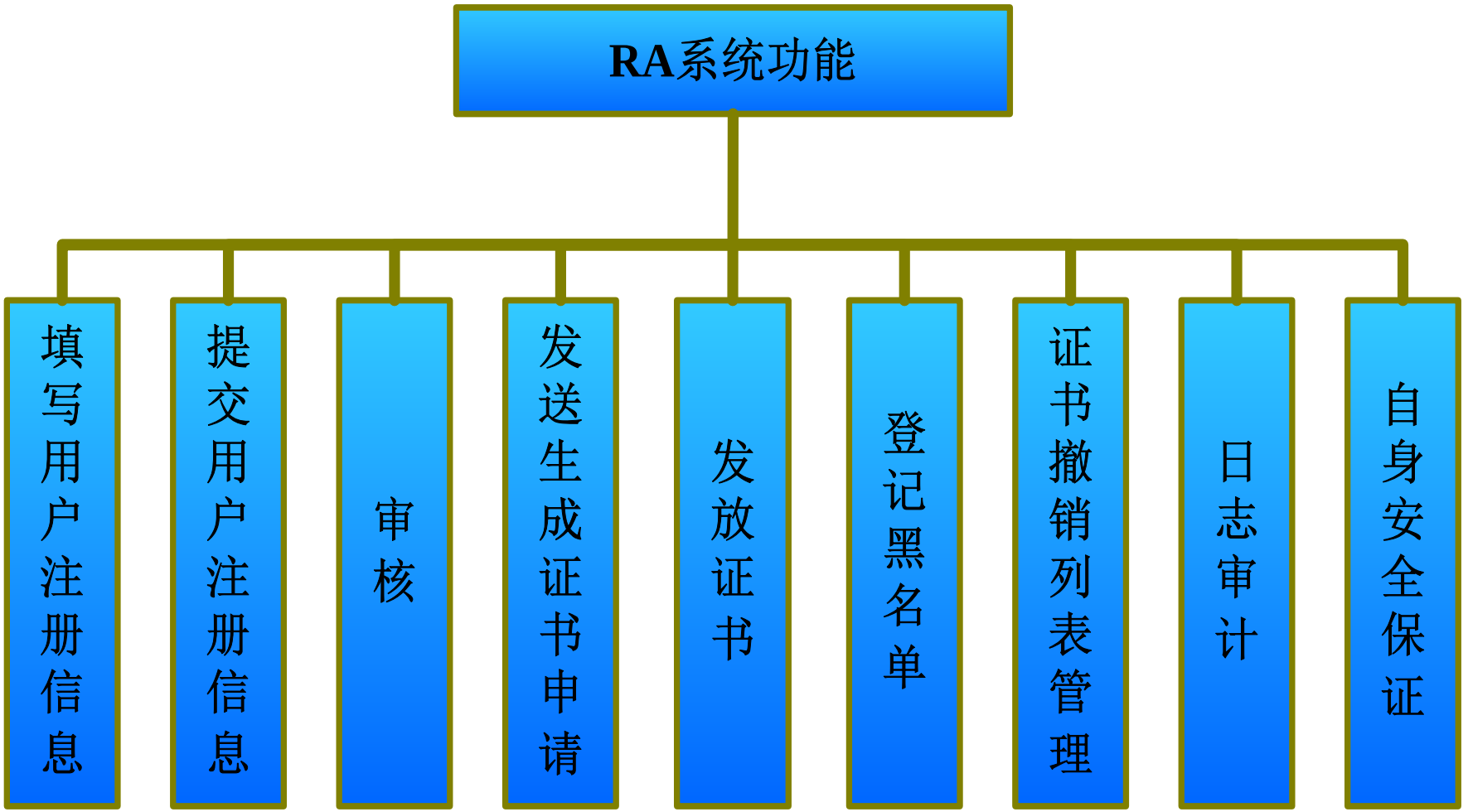
9.1 PKI的基本概念

注册机构RA

- 注册机构（RA）是数字证书注册审批机构，是认证中心的延伸。
- RA按照政策与管理规范对用户的资格进行审查，并执行“是否同意给该申请者发放证书、撤销证书”等操作。

9.1 PKI的基本概念

注册机构RA的功能



9.1 PKI的基本概念

证书发布库

用于集中存放CA颁发证书和证书撤销列表。

支持分布式存放，以提高查询效率。

LDAP协议是创建高效的大规模PKI认证的关键技术。

9.1 PKI的基本概念

密钥备份和恢复

- 仅备份和恢复CA的加/解密密钥，而不备份用户的签名密钥。

- 若用户声明公/私钥对是用于数据加密的，则CA即可对该用户的私钥进行备份。当用户丢失密钥后，可通过可信任的密钥恢复中心或CA完成密钥恢复。

3.1 PKI的基本概念

证书撤销的两种实现方法

（1）周期性发布机制

证书撤销列表CRL（Certificate Revocation List）

（2）在线证书查询机制

如在线证书状态协议OCSP（Online Certificate Status Protocol）

9.1 PKI的基本概念

PKI的应用

一 认证服务

二 数据完整性服务

三 数据保密性服务

四 不可否认服务

五 公证服务

第9章 数字证书与公钥基础设施

一 PKI的基本概念

二 数字证书

三 PKI体系结构—PKIX模型

四 PKI实例

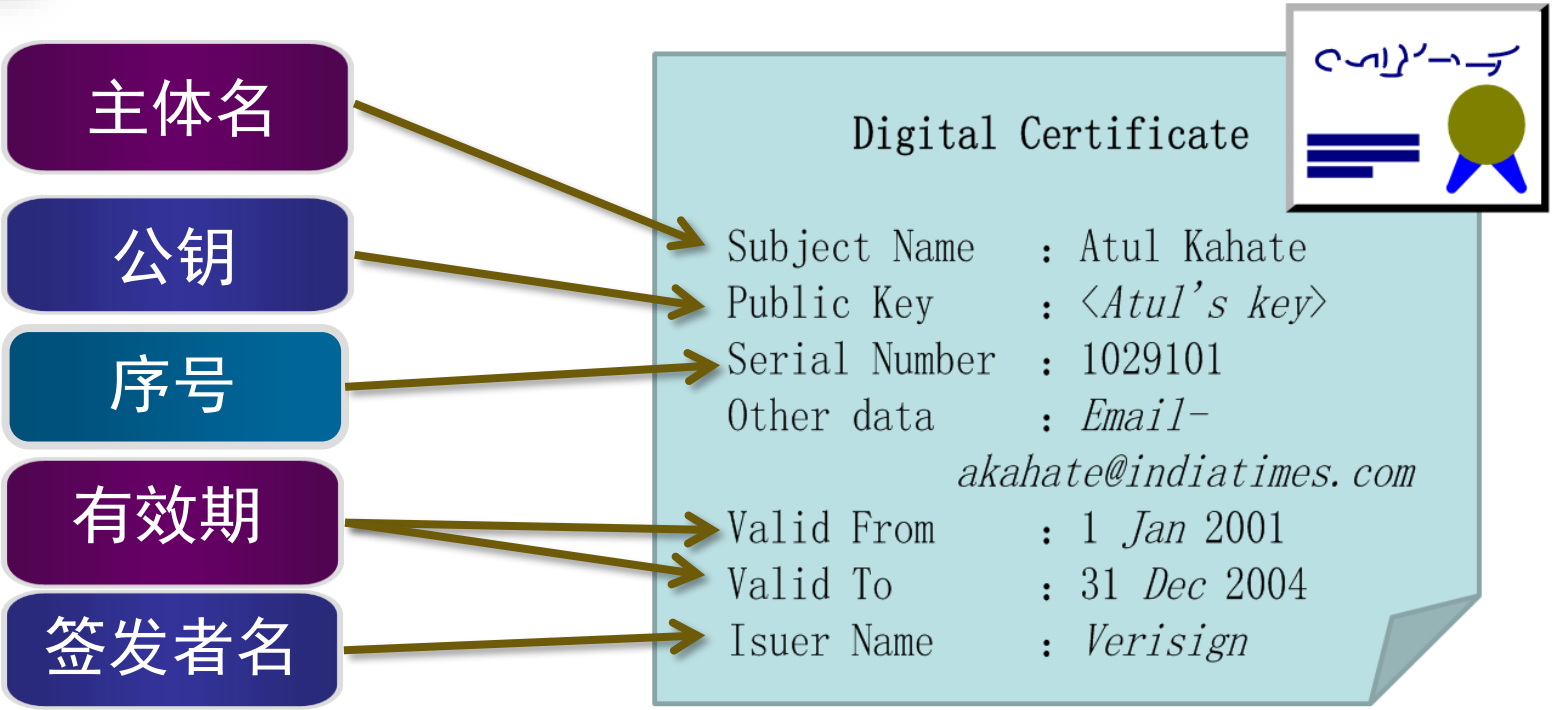
五 授权管理设施—PMI

9.2 数字证书

数字证书的概念： 将用户的身份ID与其所持有的公钥PK绑定，再由CA对该用户身份及对应公钥的组合{ID||PK}进行数字签名得到S，然后将{签名S||身份ID||公钥PK}加以存储，即数字证书。

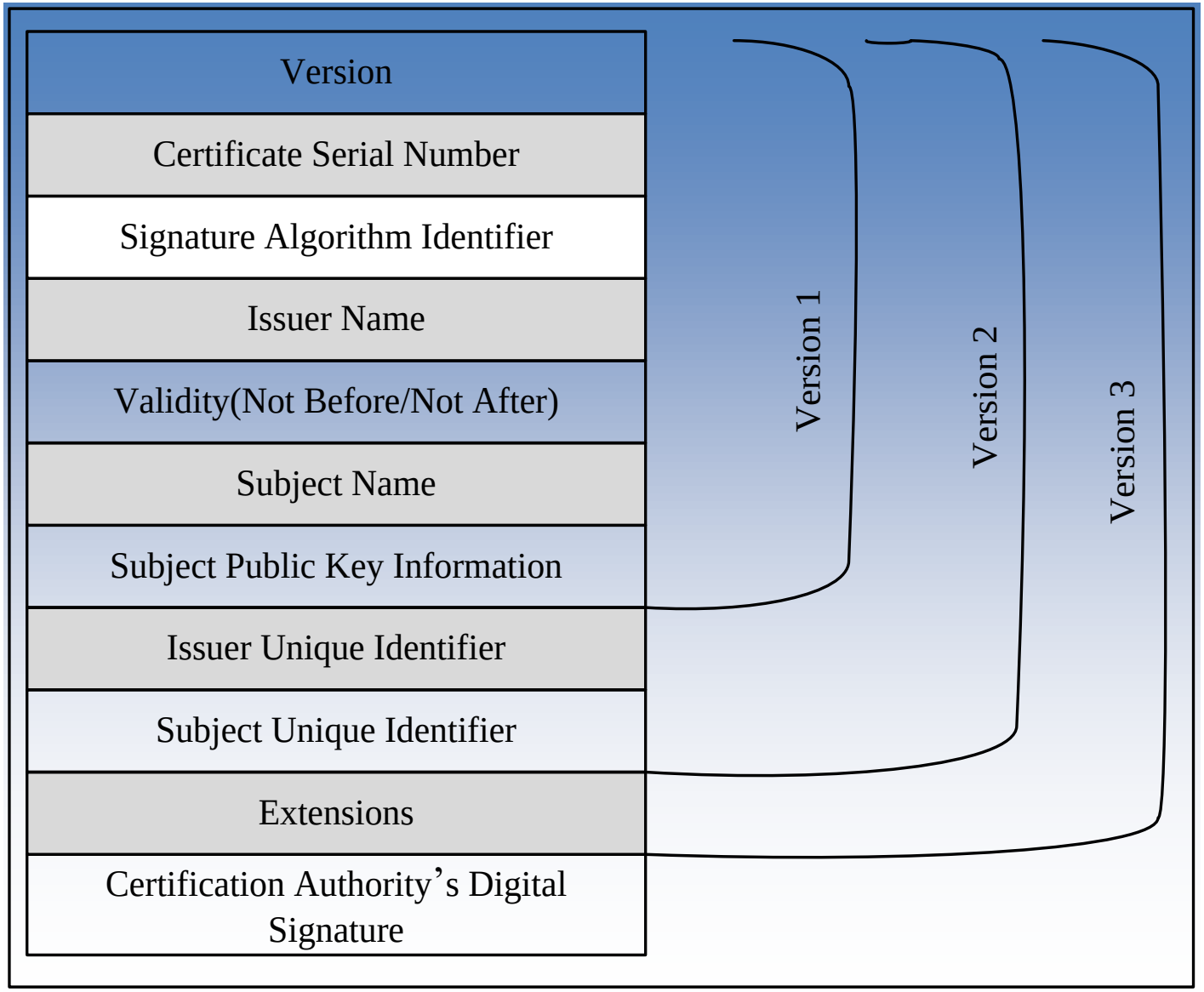
包含的信息

- 主体名
- 公钥
- 序号
- 有效期
- 签发者名

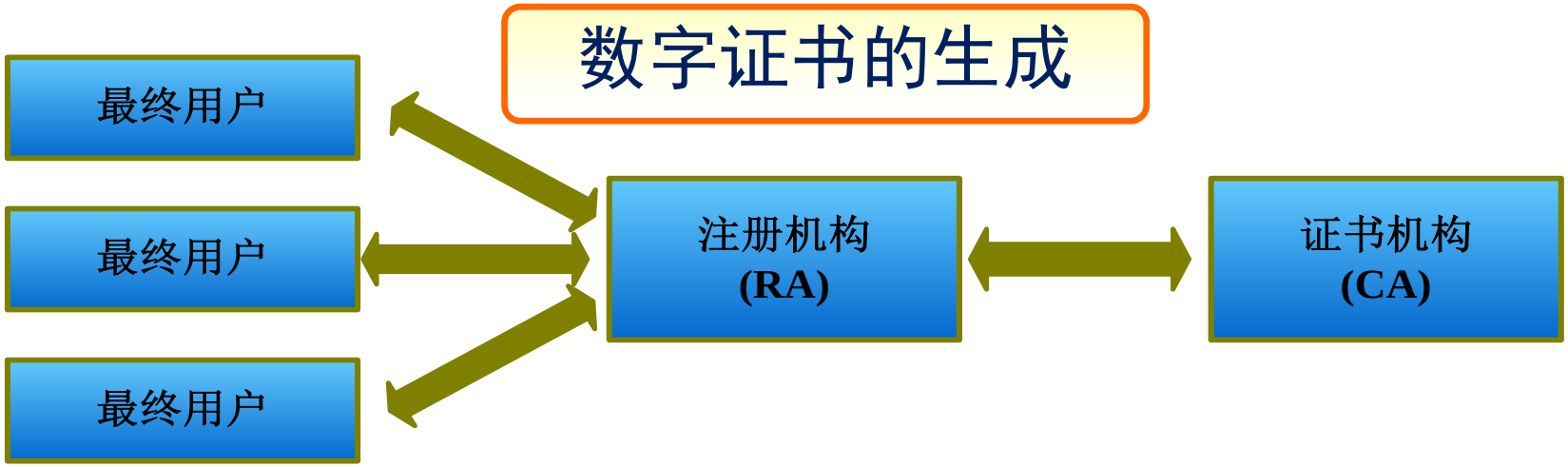


9.2 数字证书

数字证书的结构



9.2 数字证书



注册机构

提供服务：

- 接收与验证最终用户的注册信息
- 为最终用户生成密钥
- 接收与授权证书撤销请求

证书机构

提供服务：

- 负责为用户生成数字证书
- 负责为用户颁发数字证书

9.2 数字证书

数字证书的生成步骤

1. 密钥生成

2. 用户注册

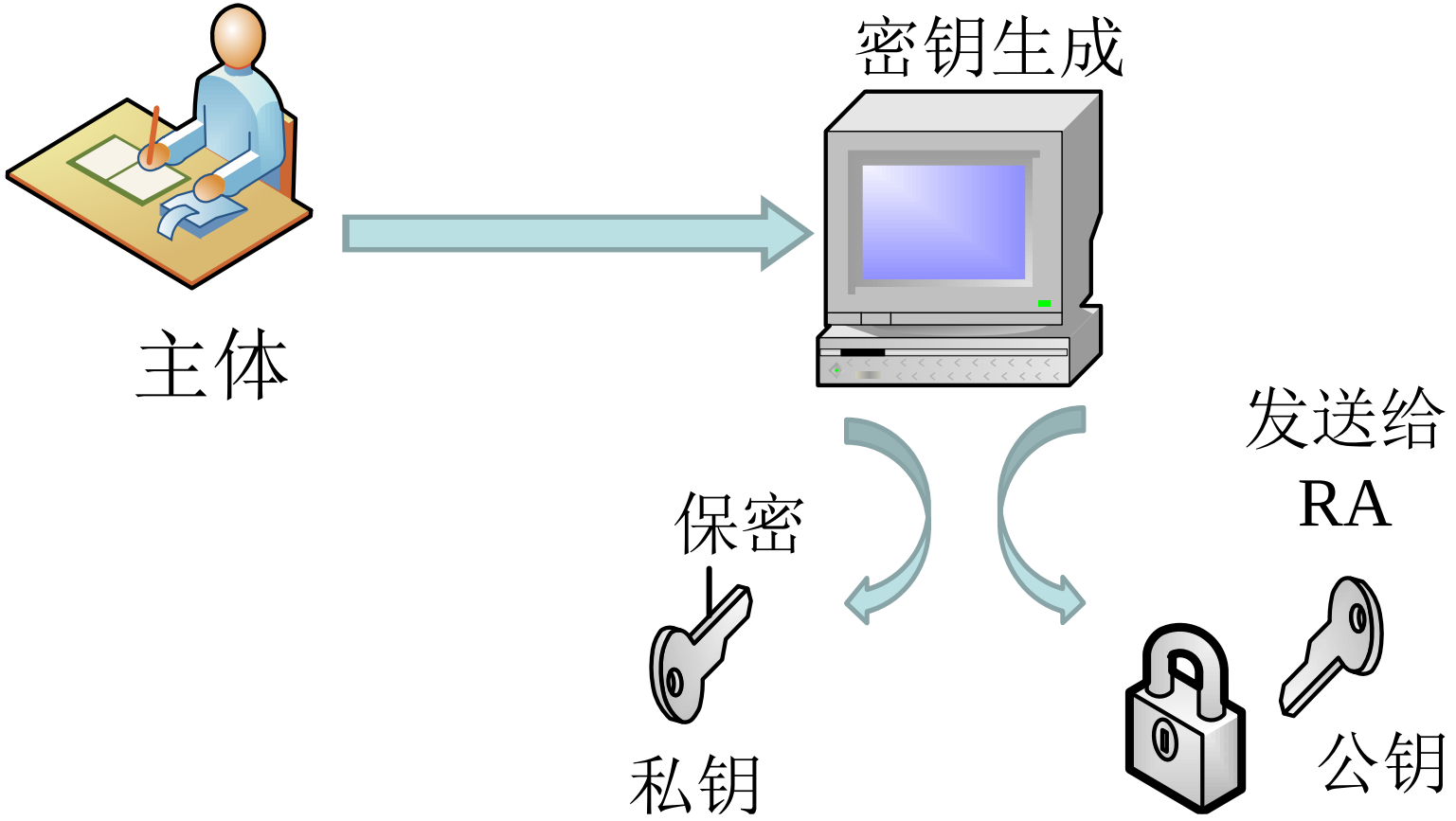
3. 验证信息

4. 证书生成

9.2 数字证书

第一步：密钥生成

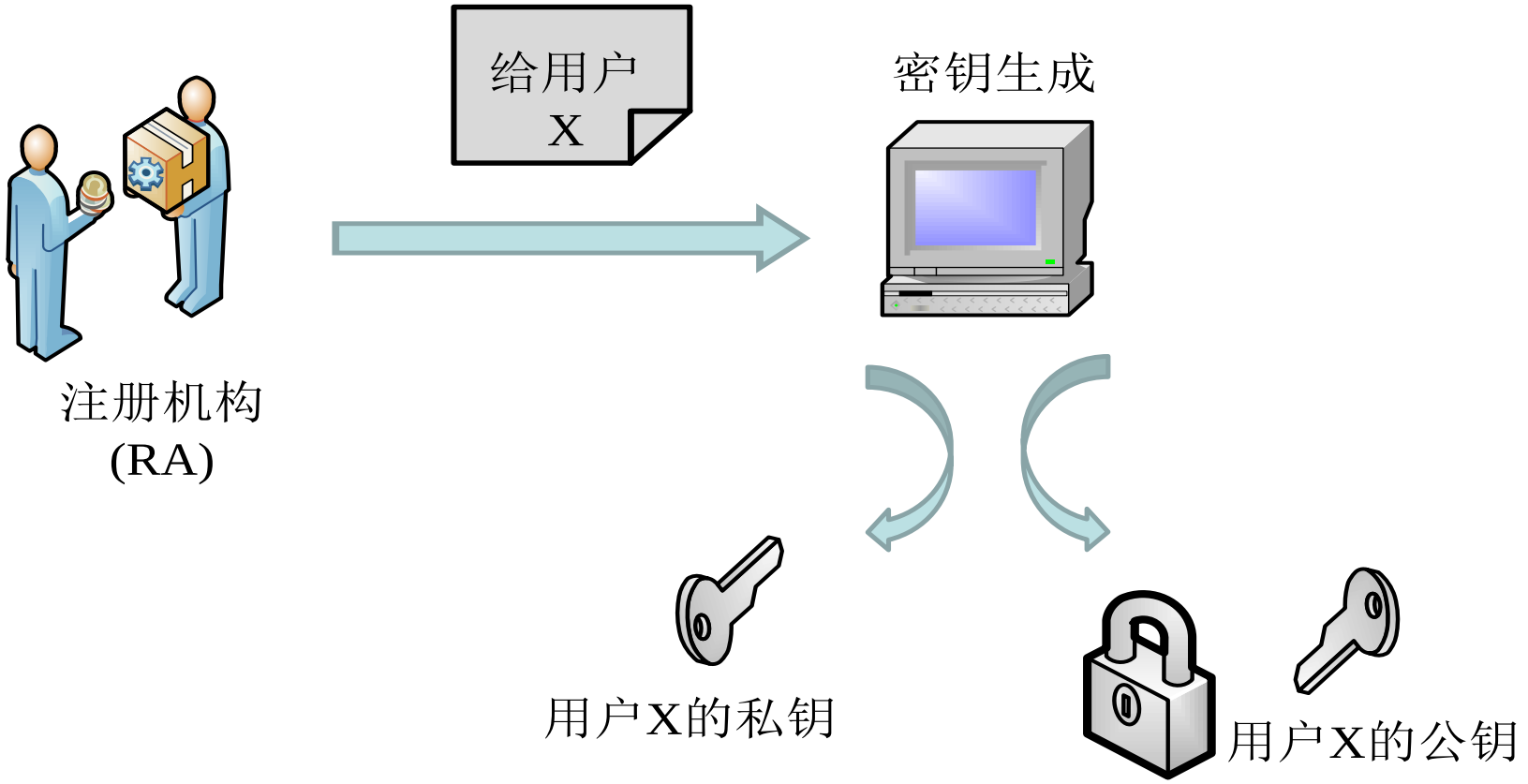
(1) 由用户自己生成公钥/私钥对



9.2 数字证书

第一步：密钥生成

(2) 注册机构为用户生成密钥对



9.2 数字证书

第二步：注册

证书申请结构

- 证书申请信息
  - 版本
  - 主体名
  - 公开密钥信息
  - 属性
- 签名算法
- 签名

用户将公钥与证明材料发送给注册机构

9.2 数字证书

第三步：验证信息

1. RA验证用户材料，以明确是否接受用户注册
2. 检查私钥的拥有证明POP（Proof Of Possession）

- RA要求用户采用私钥对证书签名请求进行数字签名。
- RA生成随机数挑战信息，用该用户公钥加密，并将加密后的挑战值发送给用户。若用户能用其私钥解密，则验证通过。

9.2 数字证书

第四步：证书生成

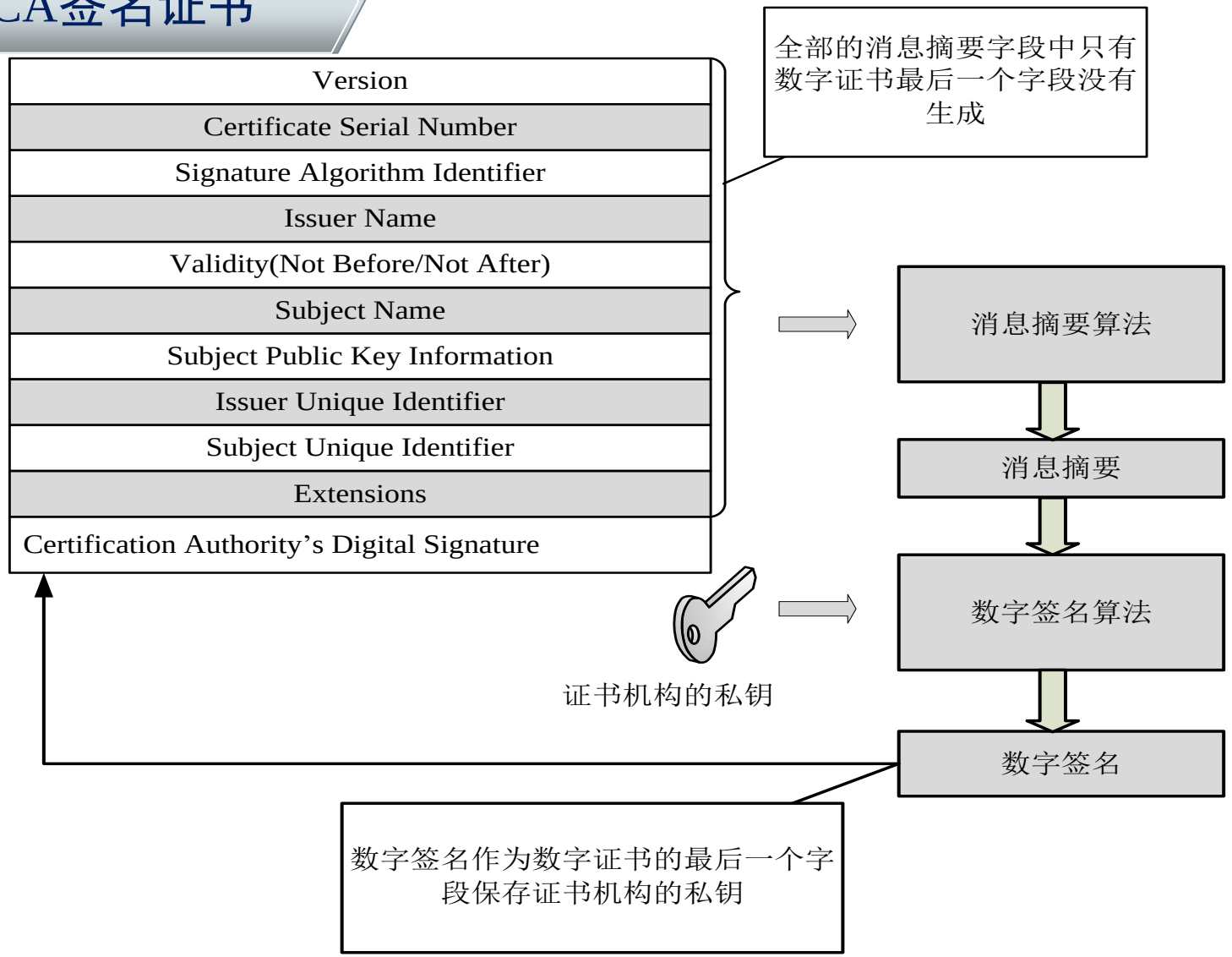
- RA将用户申请数据信息传递给证书机构CA
- 证书机构验证后生成数字证书
- 证书机构将证书发给用户
- 在CA维护的证书目录中保留一份证书记录

- RA将数字证书采用用户公钥加密后，发送给用户。
- 用户需要用与公钥匹配的私钥解密方可取得明文证书。

9.2 数字证书

(1) CA签名证书

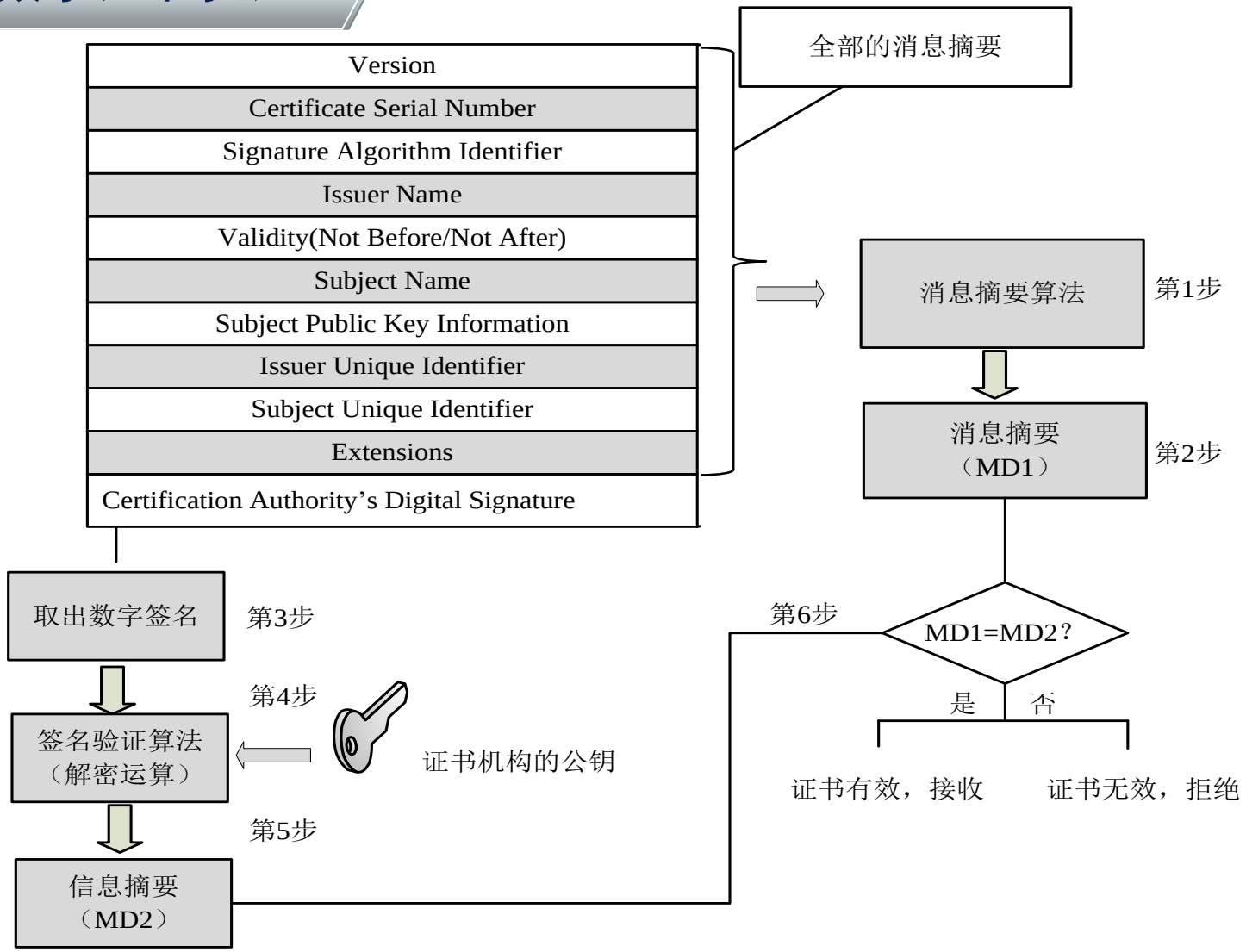
数字证书的签名与验证



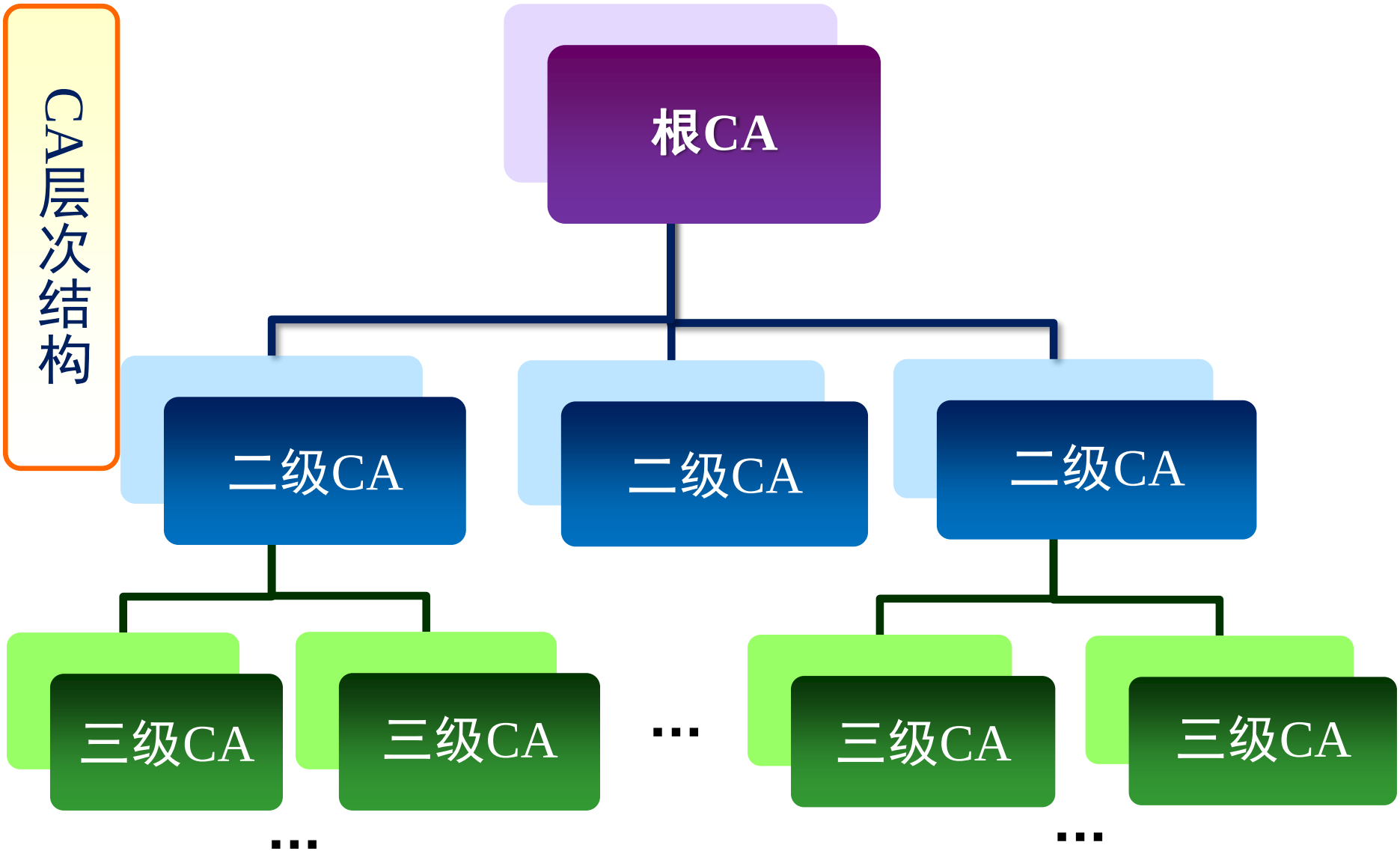
9.2 数字证书

(2) 数字证书验证

数字证书的签名与验证

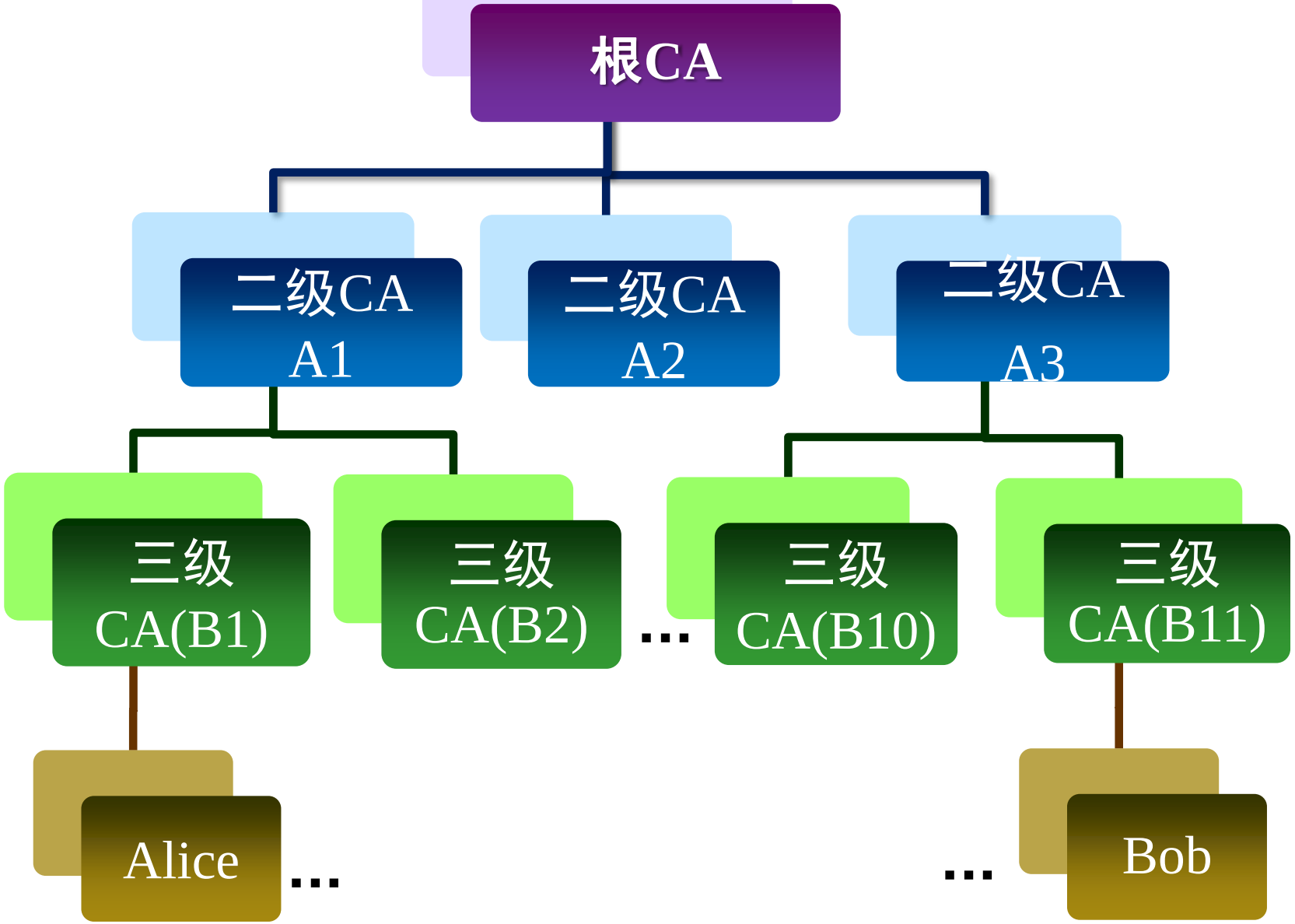


9.2 数字证书



9.2 数字证书

同一根CA中不同CA所辖用户



9.2 数字证书

验证证书链的过程

Alice

Bob

第2步： 需要B11的证书来验证Bob的证书

Bob的数字证书

第1步： 证明公钥——数字证书

第4步： 需要A3的证书来验证B11的证书

B11的数字证书

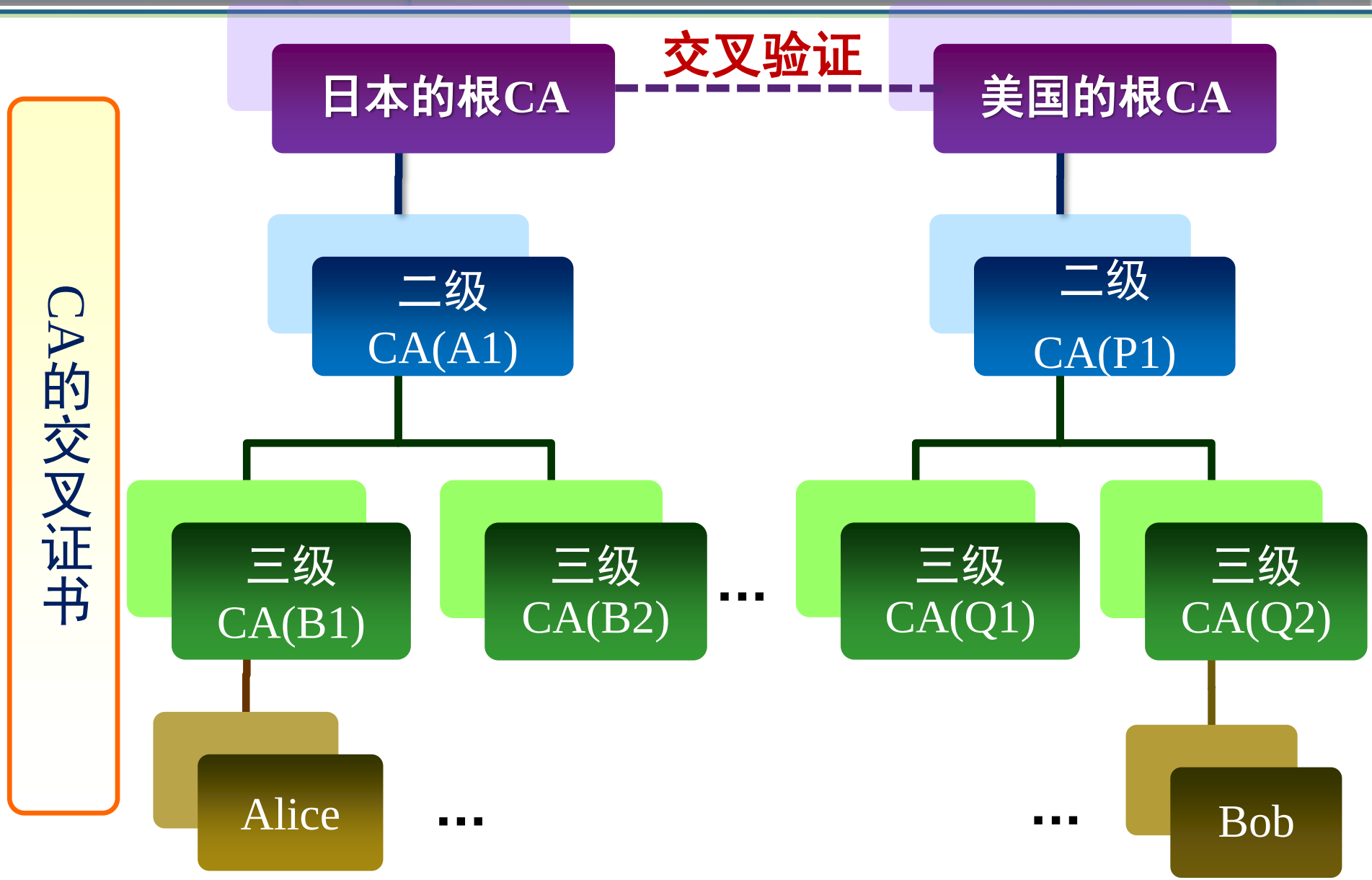
第3步： B11的证书

第6步： A3的CA是根CA，Alice已信任根CA，这就足够了

A3的数字证书

第5步： A3的证书

9.2 数字证书


交叉验证
日本的根CA
美国的根CA
CA的交叉证书
二级
CA(A1)
二级
CA(P1)
三级
CA(B1)
三级
CA(B2)
...
三级
CA(Q1)
三级
CA(Q2)
Alice
...
...
Bob

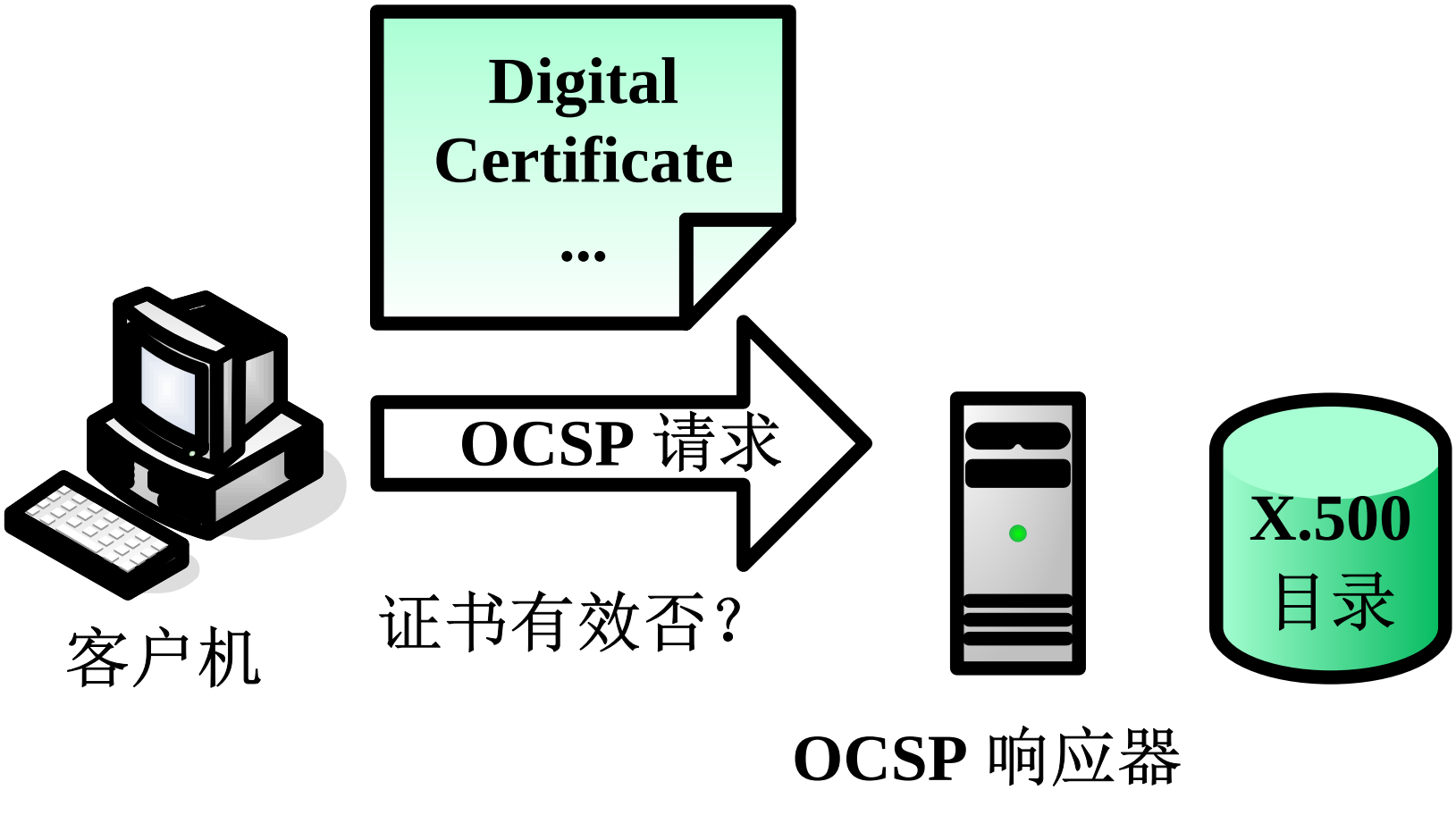
9.2 数字证书

证书撤销状态检查机制

9.2 数字证书

联机证书撤销状态检查

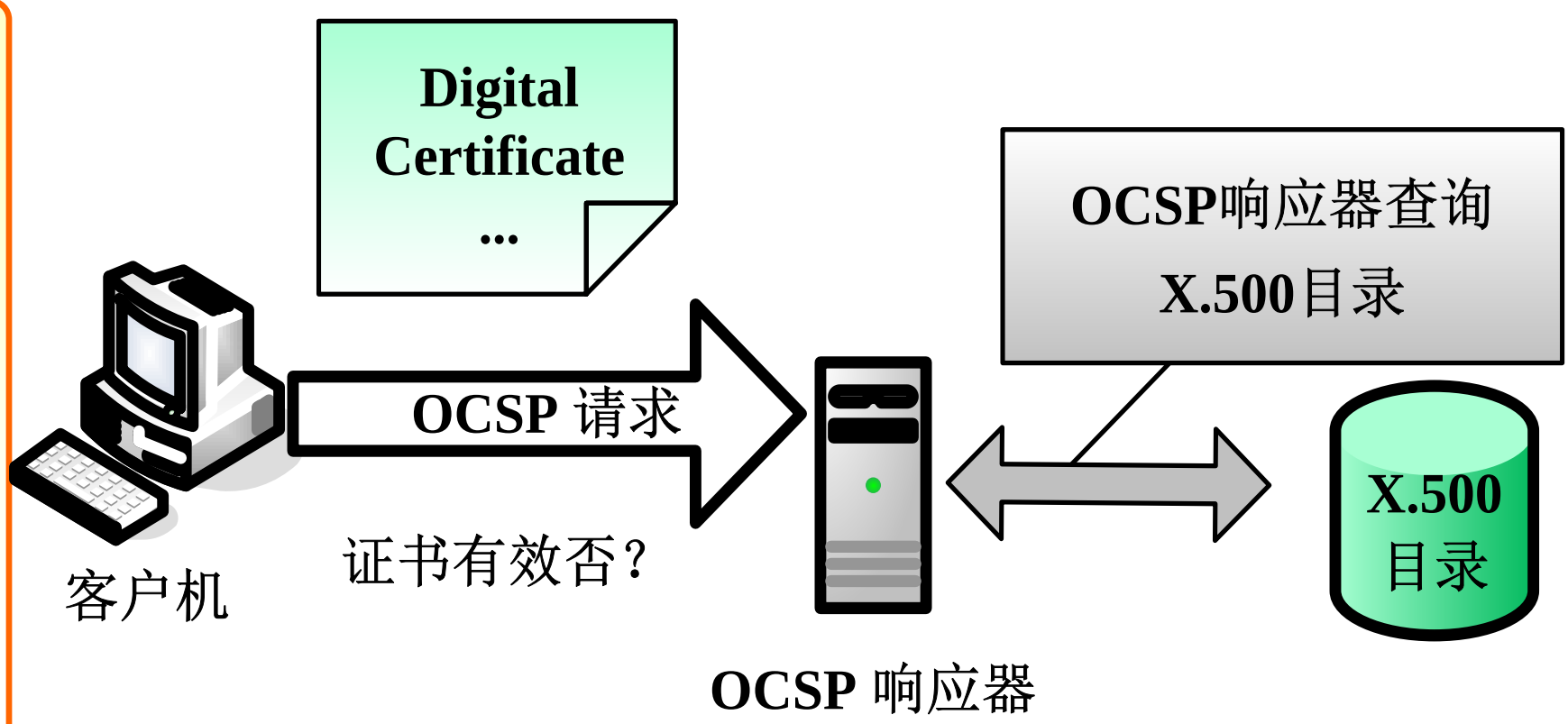
OCSP请求



9.2 数字证书

联机证书撤销状态检查

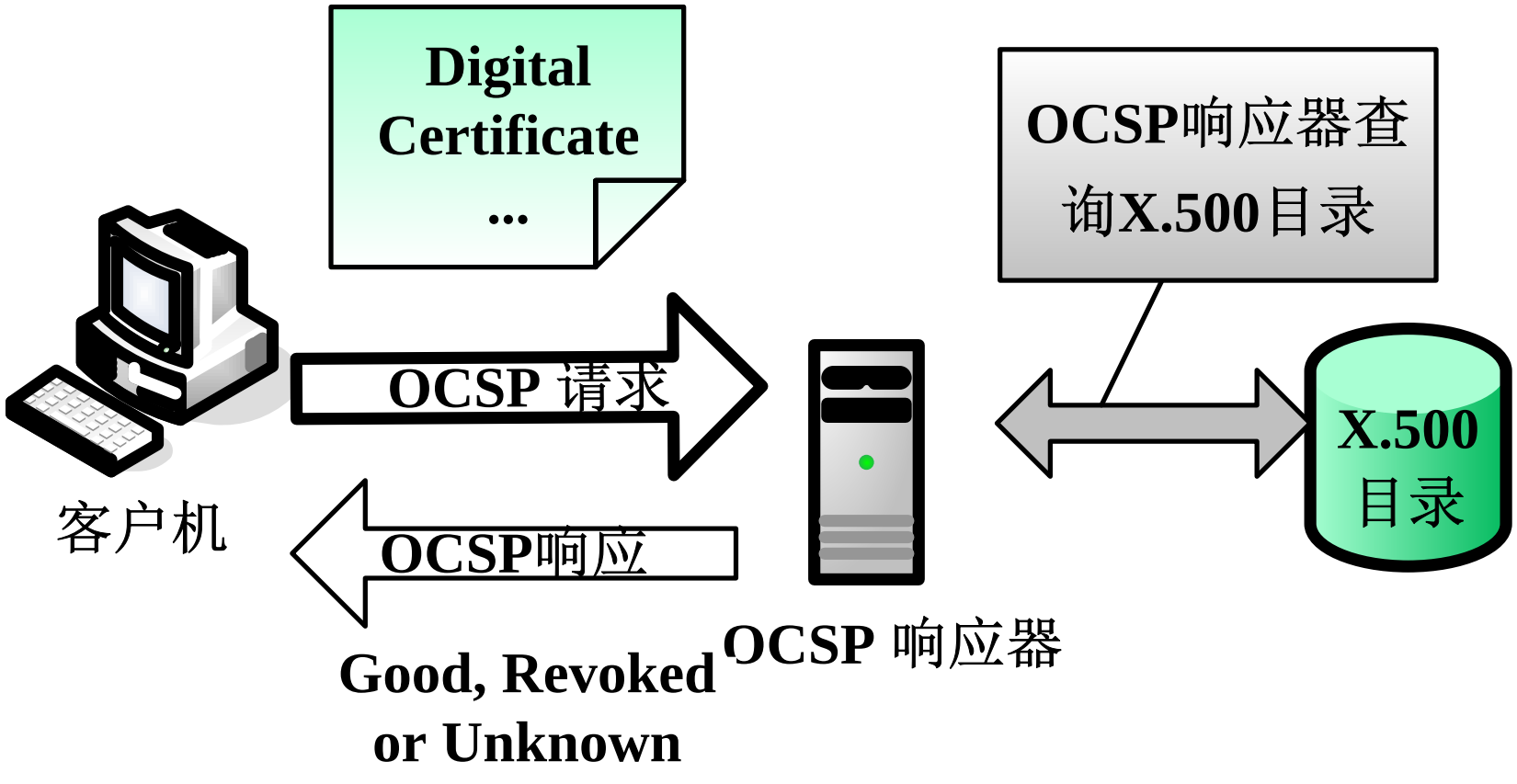
OCSP证书撤销状态检查



9.2 数字证书

联机证书撤销状态检查

OCSP响应



第9章 数字证书与公钥基础设施

一 PKI的基本概念

二 数字证书

三 PKI体系结构—PKIX模型

四 PKI实例

五 授权管理设施—PMI

9.3 PKI体系结构——PKIX模型

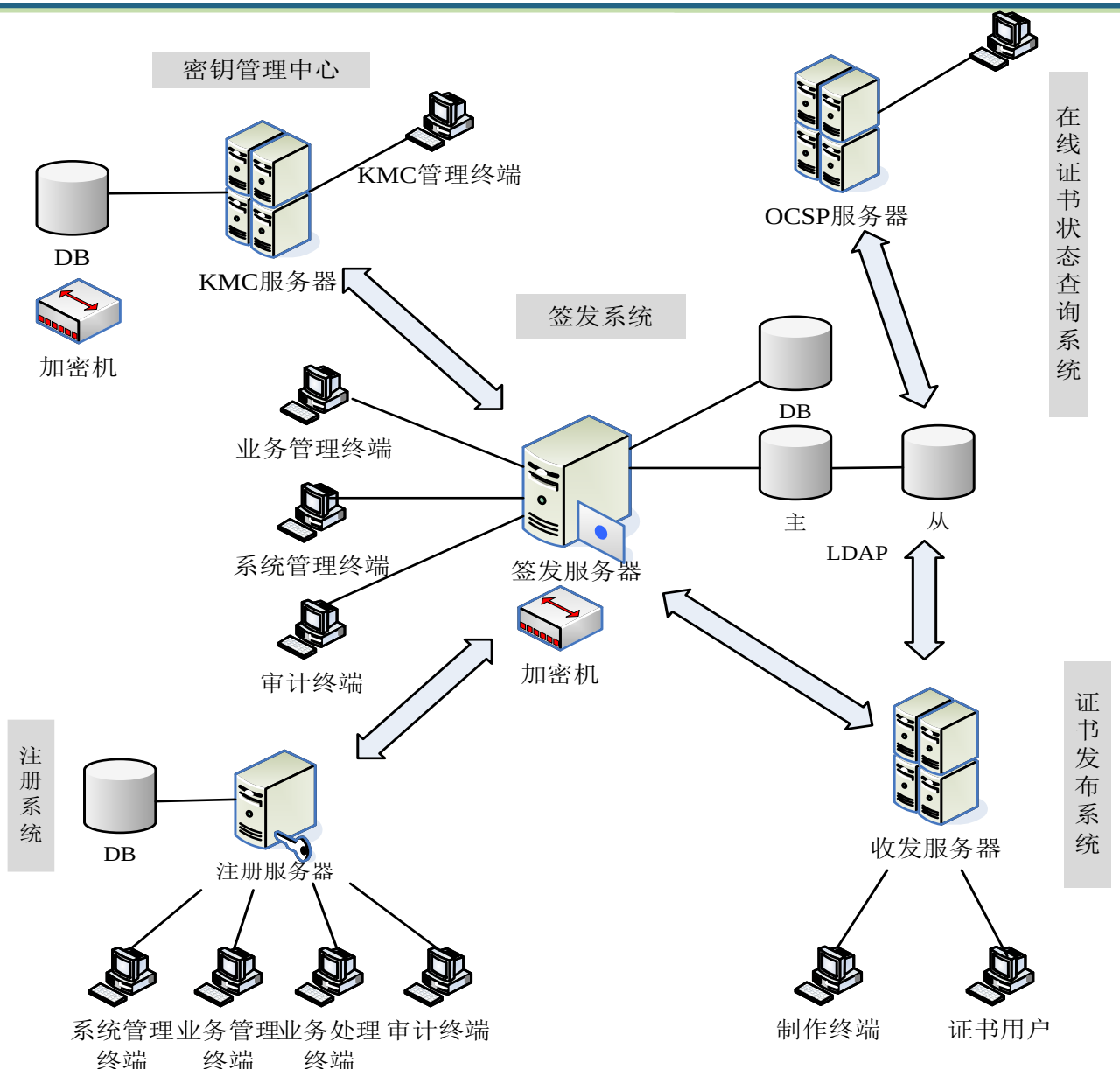
9.3 PKI体系结构——PKIX模型

◆PKIX模型采用X.509 v3的证书格式

操作协议	定义基础协议，向PKI用户发布证书、CRL和其他管理与状态信息的传输机制。
管理协议	这些协议支持不同PKI实体交换信息
策略大纲	定义了生成证书策略之类的文档，确定对于特定应用领域选择证书类型时要考虑的重点。
时间标注与数字证书服务	时间标注服务和数据证书服务（DCS）验证所收到数据的正确性，类似于日常生活中的公证方。

9.3 PKI体系结构——PKIX模型

PKI系统的拓扑结构



第9章 数字证书与公钥基础设施

一 PKI的基本概念

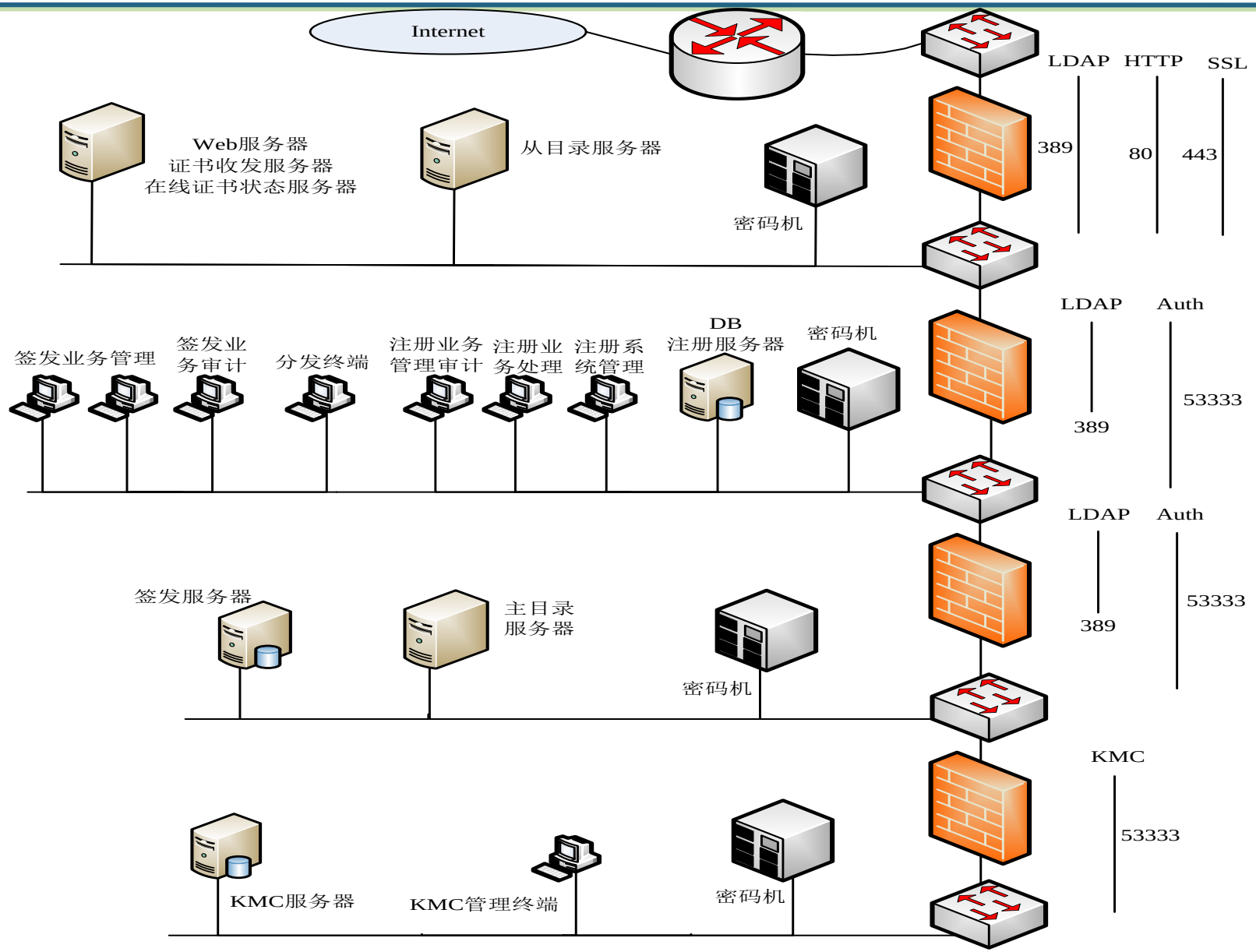
二 数字证书

三 PKI体系结构—PKIX模型

四 PKI实例

五 授权管理设施—PMI

9.4 PKI实例


Internet
LDAP
HTTP
SSL
Web服务器
证书收发服务器
在线证书状态服务器
从目录服务器
密码机
389
80
443
LDAP
Auth
签发业务管理
签发业务审计
分发终端
注册业务管理审计
注册业务处理
注册系统管理
DB
注册服务器
密码机
389
53333
LDAP
Auth
签发服务器
主目录服务器
密码机
389
53333
KMC
KMC服务器
KMC管理终端
密码机
53333

谢谢！