第4章
数字证书与公钥基础设施

中国科学技术大学
曾凡平
billzeng@ustc.edu.cn

PKI的背景

- 使用公钥密码体制的前提是通信双方**确信拥有对方的公钥**。然而，通信双方很难直接获得对方的公钥。考虑如下场景：
  - Bob和Alice生成各自的一对公/私钥，各自保存私钥，借助网络把公钥发送给对方。
  - Bob用Alice的公钥加密一个文件并发送给Alice。
  - Alice用私钥解密文件，获得原始文件
- 问题：如果入侵者监视Bob和Alice的**网络通信信道**并用自己的公钥替换Alice的**公钥！……**
- 解决方案：采用基于**可信第三方**的***PKI***

内容提要

- 公开密钥基础设施(PKI - Public Key Infrastructure)是一个用非对称密码算法原理和技术实现并提供安全服务的具有通用性的安全基础设施。
- PKI的主要目的是通过自动管理密钥和数字证书，为用户建立一个安全的网络运行环境，使用户可以在多种应用环境下采用加密和数字签名技术，保证网上数据的机密性、完整性和不可抵赖性。
- 概括地说，PKI是创建、管理、存储、分发和撤销基于公钥加密的数字证书所需要的一套硬件、软件、策略和过程的集合。

主要内容

1. PKI的基本概念
2. 数字证书
3. PKI体系结构—PKIX模型
4. PKI实例

参考：《网络安全概论》第1版

– 刘建伟 毛剑 胡荣磊，电子工业出版社，2009年07月。 第3章 数字证书与公钥基础设施

4.1 PKI的基本概念

4.1.1 PKI的定义

- PKI是一种遵循标准的利用公钥理论和技术建立的提供安全服务的基础设施。
- 所谓基础设施，就是在某个大型环境下普遍适用的基础和准则，只要遵循相应的准则，不同实体即可方便地使用基础设施所提供的服务。
- 公钥基础设施的目的是从技术上解决网上身份认证、电子信息的完整性和不可抵赖性等安全问题，为网络应用(如浏览器、电子邮件、电子交易)提供可靠的安全服务。 PKI是遵循标准的密钥管理平台，能为所有网络应用透明地提供采用加密和数字签名等密码服务所需的密钥和证书管理。

PKI的任务

- PKI**最主要的任务是确立可信任的数字身份**，这些身份可被用来和密码机制相结合，提供认证、授权或数字签名验证等服务，而使用该类服务的用户可在一定程度确信自己的行为未被误导。这一**可信的数字身份通过数字证书(也称公钥证书)来实现。数字证书(如X.509证书)是用户身份与其所持公钥的结合。**
- 在实际应用中，PKI体系在安全、易用、灵活、经济的同时，必须充分考虑互操作性和可扩展性。
- PKI体系的**功能模块**需有机结合；此外，安全应用程序的开发者不必再关心复杂的数学模型和运算，只需直接按照标准使用API**接口**即可实现相应的安全服务。

4.1.2 PKI的组成

(1) 证书机构(CA，Certificate Authority)

- PKI系统的关键是实现密钥管理。目前较好的密钥管理解决方案是采取证书机制。
- 数字证书是公开密钥体制的一种密钥管理媒介。数字证书是一种具有权威性的电子文档，其作用是证明证书中所列用户身份与证书中所列公开密钥合法且一致。要证明其合法性，就需要有可信任主体对用户证书进行公证，证明主体的身份及其与公钥的匹配关系，证书机构即是这样的可信任机构。
- CA也称数字证书认证中心(认证中心)，作为具有权威性、公正性的第三方可信任机构，是PKI体系的核心构件。CA负责发放和管理数字证书，其作用类似于现实生活中的证件颁发部门，如护照办理机构。

- **CA提供网络身份认证服务、负责证书签发及签发后证书生命周期中的所有方面的管理**，包括跟踪证书状态且在证书需要撤销(吊销)时发布证书撤销通知。CA还需维护证书档案和证书相关的审计，以保障后续验证需求。CA系统的功能如图1所示。

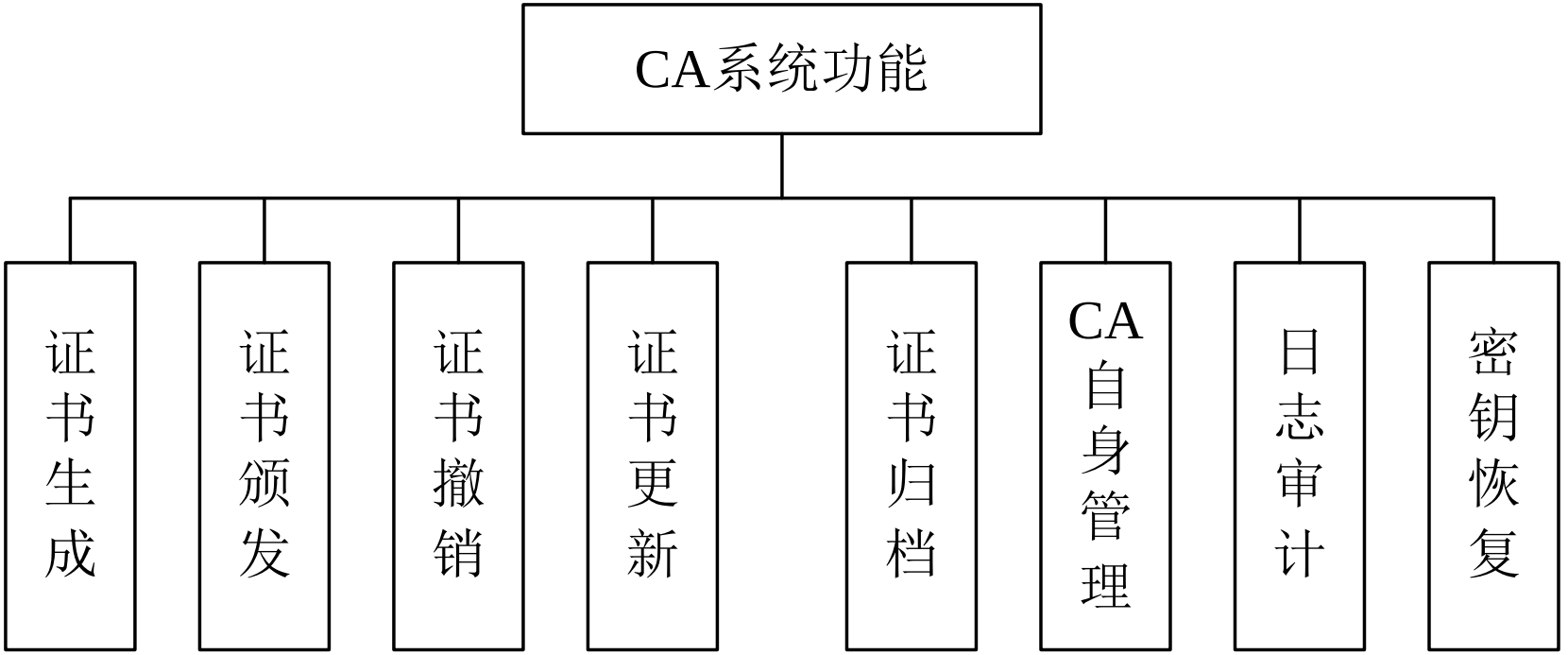
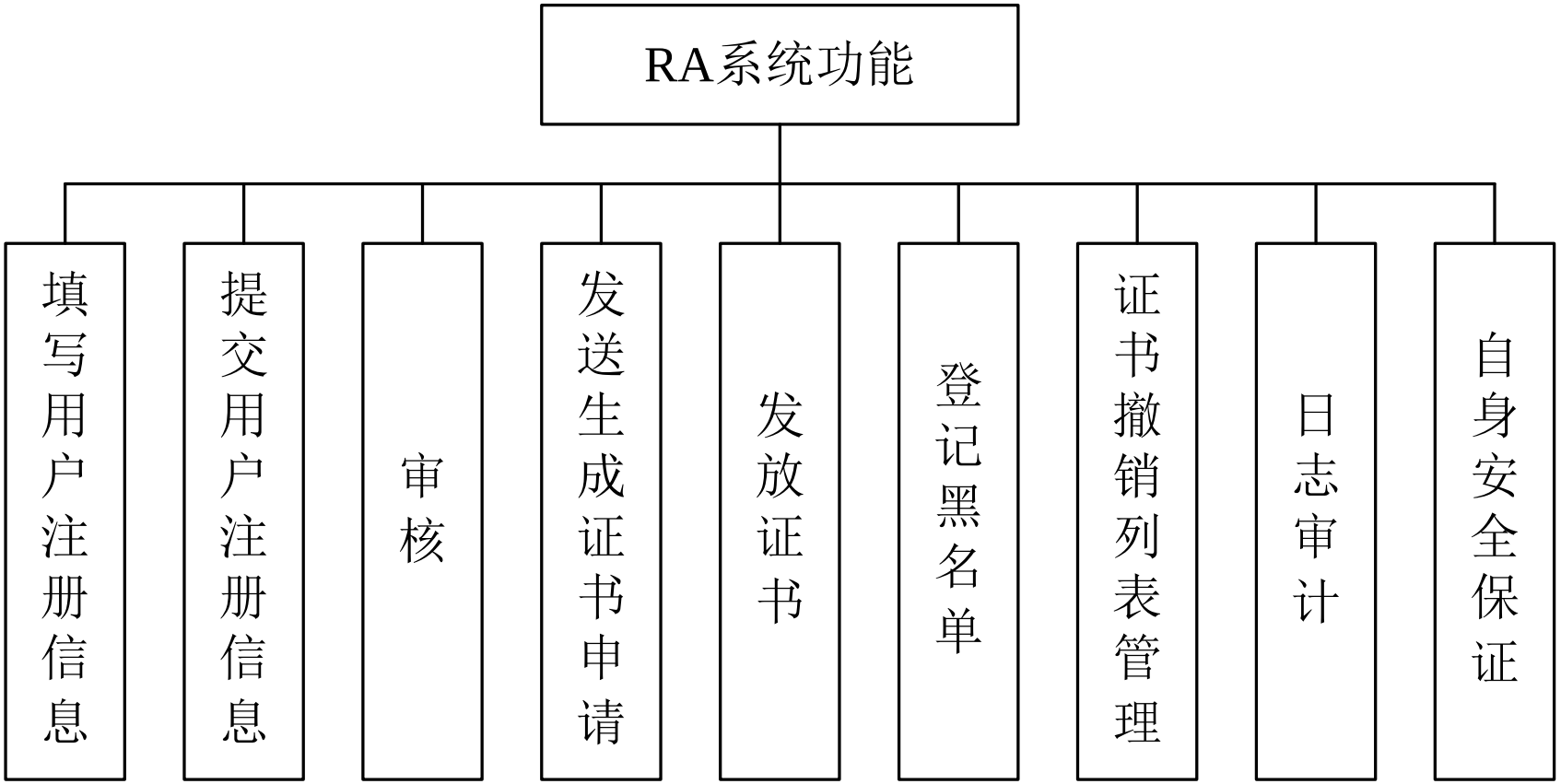


图1 CA的功能

(2) 注册机构(RA，Registration Authority)

- **注册机构(也称注册中心)是数字证书注册审批机构，**是认证中心的延伸，**与CA在逻辑上是一个整体，**执行不同的功能。RA按照特定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，承担因审核错误而引起的一切后果。如果审核通过，即可实时或批量地向CA提出申请，要求为用户签发证书。RA并不发出主体的可信声明(证明)，只有证书机构有权颁发证书和撤销证书。RA将与具体应用的业务流程相联系，是最终客户和CA交互的纽带，是整个CA中心得以运作的不可缺少的部分。
- **RA负责对证书申请进行资格审查**，其主要功能如下。

图2 RA系统的功能


RA系统功能
填写用户注册信息
提交用户注册信息
审核
发送生成证书申请
发放证书
登记黑名单
证书撤销列表管理
日志审计
自身安全保证

(1)**填写用户注册信息**：替用户填写有关用户证书申请信息。

(2)**提交用户注册信息**：核对用户申请信息，决定是否提交审核。

(3)**审核**：对用户的申请进行审核，决定“批准”还是“拒绝”用户的证书申请。

(4)**发送生成证书申请**：向CA提交生成证书请求。

(5)**发放证书**：将用户证书和私钥发放给用户。

(6)**登记黑名单**：对过期的证书和撤销的证书及时登记，并向CA发送。

(7)**证书撤销列表管理**：确保CRL的及时性，并对CRL进行管理。

(8)**日志审计**：维护RA的操作日志。

(9)**自身安全保证**：保障服务器自身密钥数据库信息、相关配置文件安全。

PKI的组成: (3) 证书发布库

- **证书发布库(简称证书库)集中存放CA颁发的证书和证书撤销列表**(CRL，Certificate Revocation List)。证书库是网上可供公众进行开放式查询的公共信息库。公众查询目的通常有两个：①得到与之通信的实体的公钥；②验证通信对方的证书是否在“黑名单”中。
- 在轻量级目录访问协议(LDAP，Lightweight Directory Access Protocol)尚未出现以前，通常由各应用程序使用各自特定的数据库来存储证书及CRL，并使用各自特定的协议实现访问。

- 这种方案存在很大的局限性，因为数据库和访问协议的**不兼容性**，使得人们无法使用其他应用程序实现对证书及CRL的访问。
- LDAP**作为一种标准的协议，使以上问题得到了解决。**此外，证书库还应该支持分布式存放，即把与本组织有关的证书和证书撤销列表存放在本地，以提高查询效率。在PKI所支持用户数量较大的情形下，PKI信息的及时性和强有力的分布机制将非常关键。LDAP目录服务支持分布式存放，是大规模PKI系统成功实施的关键，也是创建高效的认证机构的关键技术。

PKI的组成: (4) 密钥备份与恢复

- 针对用户密钥丢失的情形，PKI提供密钥备份与恢复机制。**密钥备份和恢复只能针对加/解密密钥，而无法对签名密钥进行备份**。数字签名是用于支持不可否认服务的，有时间性要求，因此不能备份/恢复签名密钥。
- 密钥备份在用户申请证书阶段进行，如果注册声明公/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。

PKI的组成: (5) 证书撤销

- 证书由于某些原因需要作废时，如用户身份姓名的改变、私钥被窃或泄露、用户与所属企业关系变更等，PKI需要使用一种方法警告其他用户不要再使用该用户的公钥证书，这种警告机制被称为证书撤销。
- 证书撤销的主要实现方法有以下两种。

1) **利用周期性发布机制**，如证书撤销列表(CRL，Certificate Revocation List)。证书撤销消息的更新和发布频率非常重要，两次证书撤销信息发布之间的间隔称为撤销延迟。在特定PKI系统中，撤销延迟必须遵循相应的策略要求。

2) **在线查询机制**，如在线证书状态协议(OCSP，Online Certificate Status Protocol)。

PKI的组成: **(6) PKI应用接口**

- PKI 研究的初衷就是让用户能方便地使用加密、数字签名等安全服务，因此一个完善的PKI 必须提供良好的应用接口系统，使得各种应用能够以**安全、一致、可信**的方式与PKI 交互，确保安全网络环境的完整性和易用性。

- PKI 应用接口系统应该是跨平台的。

4.1.3 PKI的应用

- PKI的应用非常广泛，如安全浏览器、安全电子邮件、电子数据交换、Internet上的信用卡交易及VPN等。PKI作为安全基础设施，它能够提供的主要服务如下。

(1) **认证服务**

- **认证服务即身份识别与认证，就是确认实体即为自己所声明的实体，鉴别身份的真伪。**
- 以甲乙双方的认证为例：甲首先要验证乙的证书的真伪，乙在网上将证书传送给甲，甲用CA的公钥解开证书上CA的数字签名，若签名通过验证，则证明乙持有的证书是真的；接着甲还要验证乙身份的真伪，乙可将自己的公钥用其私钥进行数字签名传送给甲，甲已从乙的证书库中查得乙的公钥，甲即可用乙的公钥来验证乙的数字签名。若该签名通过验证，乙在网上的身份就确凿无疑了。

(2) 数据完整性服务

- **数据完整性服务就是确认数据没有被修改过。**
- **实现数据完整性服务的主要方法是数字签名，它既可以提供实体验证，又可以保障被签名数据的完整性，这由杂凑算法和签名算法提供保证。**
- 杂凑算法的特点是输入数据的任何变化都会引起输出数据不可预测的极大变化，而签名是用自己的私钥将该杂凑值进行加密，然后与数据一道传送给接收方。如果敏感数据在传输和处理过程中被篡改，接收方就不会收到完整的数字签名，验证就会失败。反之，若签名通过了验证，就证明接收方收到的是未经修改的完整数据。

(3) 数据保密性服务

- **PKI的保密性服务采用了“数字信封”机制**，即发送方先产生一个对称密钥，并用该对称密钥加密数据。同时，发送方还用接收方的公钥加密该对称密钥，就像把它装入一个“数字信封”，然后把被加密的对称密钥(“数字信封”)和被加密的敏感数据一起传送给接收方。接收方用自己的私钥拆开“数字信封”，并得到对称密钥，再用对称密钥解开被加密的敏感数据。

(4) 不可否认服务

- **不可否认服务是指从技术上保证实体对其行为的认可**。在这中间，人们更关注的是数据来源的不可否认性、接收的不可否认性及接收后的不可否认性，此外还有传输的不可否认性、创建的不可否认性和同意的不可否认性。

(5) 公证服务

- PKI中的公证服务与一般社会提供的公证人服务有所不同，PKI**中支持的公证服务是指“数据认证”，也就是说，公证人要证明的是数据的有效性和正确性**，这种公证取决于数据验证的方式。例如，在PKI中被验证的数据是基于杂凑值的数字签名、公钥在数学上的正确性和签名私钥的合法性。

- PKI提供的上述**5种安全服务**能很好地满足电子商务、电子政务、网上银行、网上证券等行业的安全需求，是确保这些活动能够顺利进行的安全措施。

4.2 数字证书

4.2.1 数字证书的概念
4.2.2 数字证书的结构
4.2.3 数字证书的生成
4.2.4 数字证书的签名与验证
4.2.5 数字证书层次与自签名数字证书
4.2.6 交叉证书
4.2.7 数字证书的撤销
4.2.8 漫游证书

关于数字证书

- PKI与非对称加密密切相关，涉及消息摘要、数字签名与加密等服务。数字证书技术则是支持以上服务的PKI关键技术之一。
- 数字证书可理解为相当于护照、驾驶执照之类用以证明实体身份的证件。例如，护照可以证明实体的姓名、国籍、出生日期和地点、照片与签名等方面信息。类似地，数字证书也可以证明网络实体在特定安全应用的相关信息。
- **数字证书就是一个用户的身份与其所持有的公钥的结合，在结合之前由一个可信任的权威机构CA来证实用户的身份，然后由该机构对该用户身份及对应公钥相结合的证书进行数字签名，以证明其证书的有效性。**

4.2.1 数字证书的概念

- **数字证书实际上是一个计算机文件，该数字证书将建立用户身份与其所持公钥的关联**。其主要包含的信息有：
  ① 主体名(Subject Name)，数字证书中任何用户名均称为主体名(即使数字证书可能颁发给个人或组织)；
  ② 序号(Serial Number)；
  ③ 有效期；
  ④ 签发者名(Issuer Name)。
- 数字证书的示例如图3所示。

图3 数字证书的示例

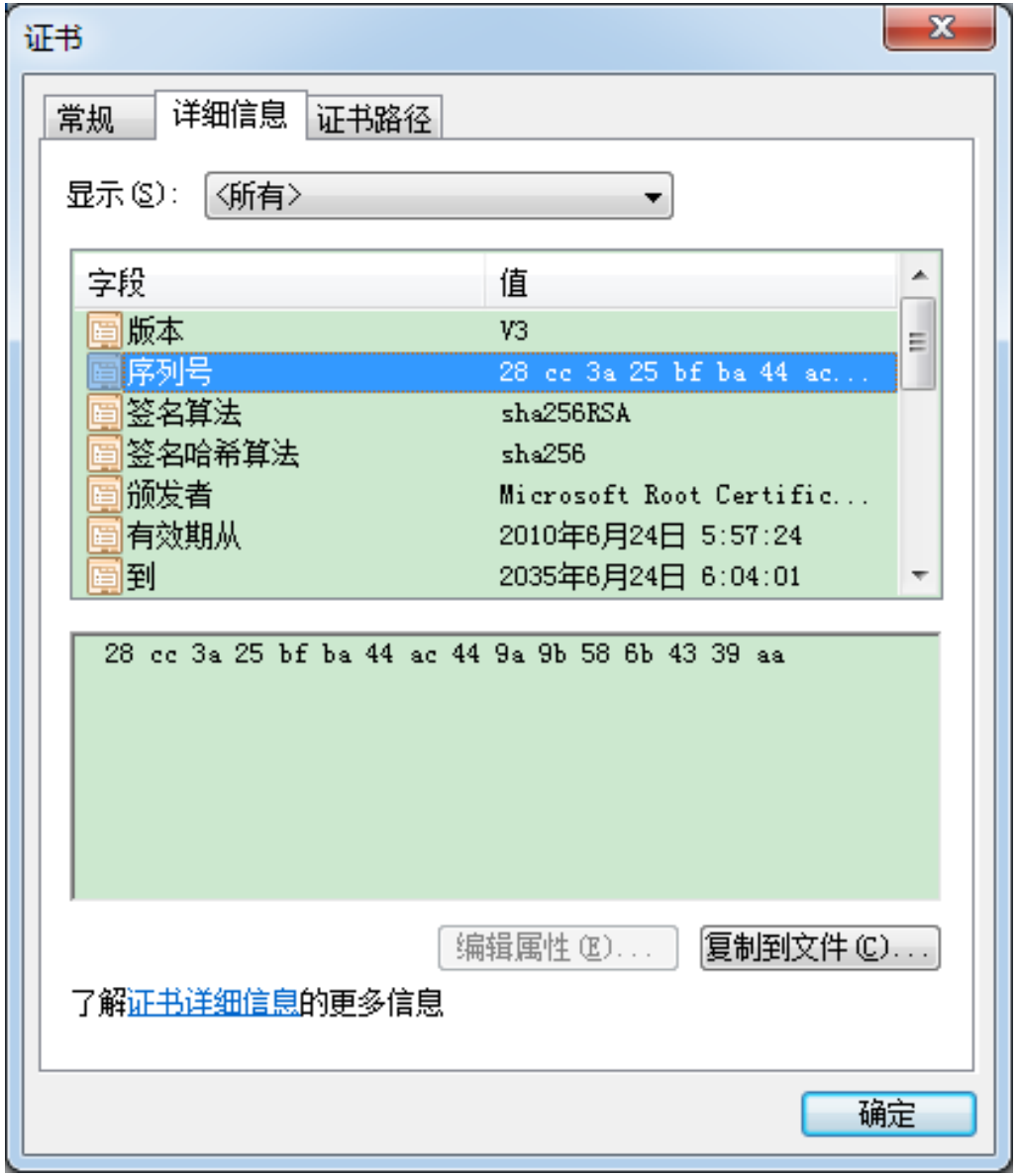

证书
常规
详细信息
证书路径
显示(S): <所有>
字段
值
版本
V3
序列号
28 cc 3a 25 bf ba 44 ac...
签名算法
sha256RSA
签名哈希算法
sha256
颁发者
Microsoft Root Certific...
有效期从
2010年6月24日 5:57:24
到
2035年6月24日 6:04:01
28 cc 3a 25 bf ba 44 ac 44 9a 9b 58 6b 43 39 aa
编辑属性(E)...
复制到文件(C)...
了解证书详细信息的更多信息
确定

表1 常规护照与数字证书项目比对

常规护照项目	数字证书项目
姓名(Full Name)	主体名(Subject Name)
护照号(Passport Number)	序(列)号(Serial Number)
起始日期(Valid From)	起始日期(Valid From)
终止日期(Valid To)	终止日期(Valid to)
签发者(Issued Name)	签发者名(Issuer Name)
照片与签名(Photograph and Signature)	公钥(Public Key)

- 由表1可见，常规护照与数字证书项目非常相似。
  - 同一签发者签发的护照不会有重号，同样，**同一签发者签发的数字证书的序号(序列号)也不会重复**。
  - 签发数字证书的机构通常为一些著名组织，世界上最著名的证书机构为VeriSign与Entrust。在国内，许多政府机构和企业也建立了自己的CA中心。例如，**我国的12家银行联合组建了CFCA(http://www.cfca.com.cn/中国金融认证中心)**。
  - 证书机构有权向个人和组织签发数字证书，使其可在非对称加密应用中使用这些证书。

4.2.2 数字证书的结构

- 国际电信联盟(ITU)于1988年推出数字证书的结构标准，当时放在X.500标准中。后来，X.509标准于1993年和1995年做了两次修订。这个标准的最新版本是X.509 v3。1999年，Internet工程任务小组(IETF)发表了X.509标准的草案RFC 2459。
- 如图4所示的是X.509 v3数字证书的结构，显示出X.509标准指定的数字证书字段，还指定了字段对应的标准版本。可以看出，X.509标准第1版共有7个基本字段，第2版增加了2个字段，第3版增加了1个字段。增加的字段分别被称为第2版和第3版的扩展或扩展属性。这些版本的末尾还有1个共同字段。表2(a)、表2(b)、表2(c)列出了这三个版本中的字段描述。

图4　X.509 v3数字证书的结构

Version	version 1	version 2	version 3
Serial Number			
Signature Algorithm Identifier			
Issuer Name			
Validity Period			
Subject Name			
Subject Public Key Information			
Issuer Unique ID			
Subject Unique ID			
Extensions			
Certification Authority's Digital Signature			

表2(a) X.509数字证书字段描述——第1版

字段	描述
版本(Version)	X.509证书版本号，目前取值1/2/3
证书序号(Serial Number)	该CA产生的证书的唯一标识号
签名算法标识符 (Signature Algorithm Identifier)	CA签名数字证书使用的算法
签名者(Issuer Name)	CA的可区分名字
有效期(之前/之后) (validity(Not Before/Not After)	该证书的有效日期，至少精确到秒
主体名(Subject Name)	证书持有者的名字
主体公钥信息 (Subject Public Key Information)	与公钥和公钥算法相关的信息

表2(b) X.509数字证书字段描述—第2版

字段	描述
签发者唯一标识符 (Issuer Unique Identifier)	在两个或多个CA使用相同签发者名时标识CA
目标唯一标识符 (Subject Unique Identifier)	在两个或多个主体使用相同签发者名时标识CA

表2(c) X.509数字证书字段描述——第3版

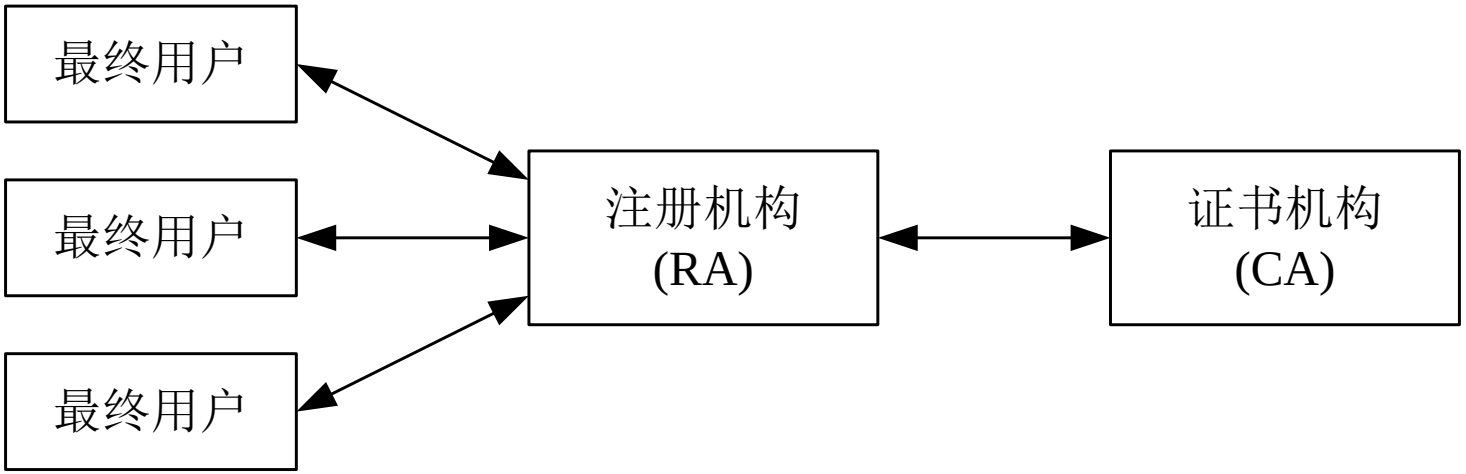
Extension	Description
Authority Key Identifier	Identifies the certification authority (CA) public key that corresponds to the CA private key used to sign the certificate.
Basic Constraints	Specifies whether the entity can be used as a CA and, if so, the number of subordinate CAs that can exist beneath it in the certificate chain.
Certificate Policies	Specifies the policies under which the certificate has been issued and the purposes for which it can be used.
CRL Distribution Points	Contains the URI of the base *certificate revocation list* (CRL).
Enhanced Key Usage	Specifies the manner in which the public key contained in the certificate can be used.
Issuer Alternative Name	Specifies one or more alternative name forms for the issuer of the certificate request.
Key Usage	Specifies restrictions on the operations that can be performed by the public key contained in the certificate.
Name Constraints	Specifies the namespace within which all subject names in a certificate hierarchy must be located. The extension is used only in a CA certificate.

Policy Constraints	Constrains path validation by prohibiting policy mapping or by requiring that each certificate in the hierarchy contain an acceptable policy identifier. The extension is used only in a CA certificate.
Policy Mappings	Specifies the policies in a subordinate CA that correspond to policies in the issuing CA.
Private Key Usage Period	Specifies a different validity period for the private key than for the certificate with which the private key is associated.
Subject Alternative Name	Specifies one or more alternative name forms for the subject of the certificate request. Example alternative forms include e-mail addresses, DNS names, IP addresses, and URIs.
Subject Directory Attributes	Conveys identification attributes such as the nationality of the certificate subject. The extension value is a sequence of OID-value pairs.
Subject Key Identifier	Differentiates between multiple public keys held by the certificate subject. The extension value is typically a SHA-1 hash of the key.

4.2.3 数字证书的生成

- **数字证书生成与管理主要涉及的参与方有：最终用户、注册机构、证书机构**。和数字证书信息紧密相关的机构有**最终用户(主体)**和**证书机构(签发者)**。
- 证书机构的任务繁多，如签发新证书、维护旧证书、撤销因故无效证书等，因此一部分证书生成与管理任务由第三方——注册机构(RA)完成。从最终用户角度看，证书机构与注册机构差别不大。技术上，注册机构是用户与证书机构之间的中间实体，如图5所示。

图5 最终用户与RA和CA的关系



- 注册机构提供的服务有：①接收与验证最终用户的**注册信息**；②为最终用户生成**密钥**；③接收与授权**密钥备份与恢复请求**；④接收与授权**证书撤销请求**。
- **注意：注册机构主要帮助证书机构与最终用户间交互，注册机构不能签发数字证书，证书只能由证书机构签发。**

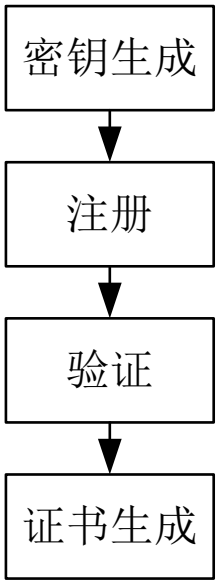
图6 数字证书的生成步骤　　图7 主体生成密钥对

- 数字证书的生成步骤如图6所示，下面对各步进行详细介绍。

第1步：密钥生成。密钥的生成可采用的方式有如下两种。

- **(1)** 主体(用户/组织)可采用特定软件生成公钥/私钥对，该软件通常是Web浏览器或Web服务器的一部分，也可以使用特殊软件程序。主体必须秘密保存私钥，并将公钥、身份证明与其他信息发送给注册机构，如图7所示。

图6



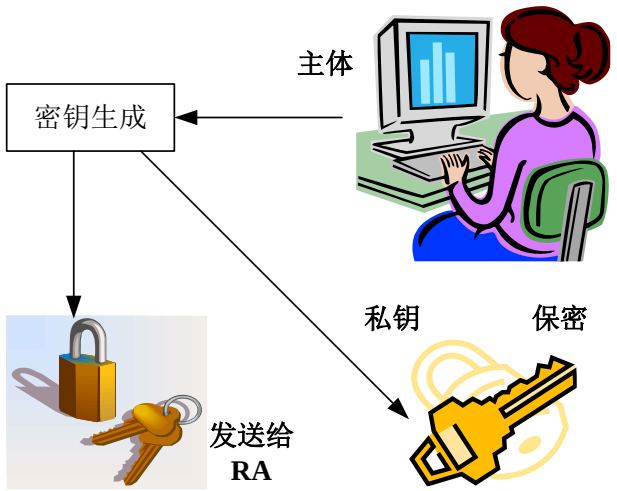


图7 主体生成密钥对

图8 注册机构主体生成密钥对示意图

- (2) 当用户不知密钥对生成技术或要求注册机构集中生成和发布所有密钥，以便于执行安全策略和密钥管理时，也可由注册机构为主体(用户)生成密钥对。该方法的缺陷是注册机构知道用户私钥，且在向主体发送途中也可能泄露。注册机构为主体生成密钥对示意图如图8所示。

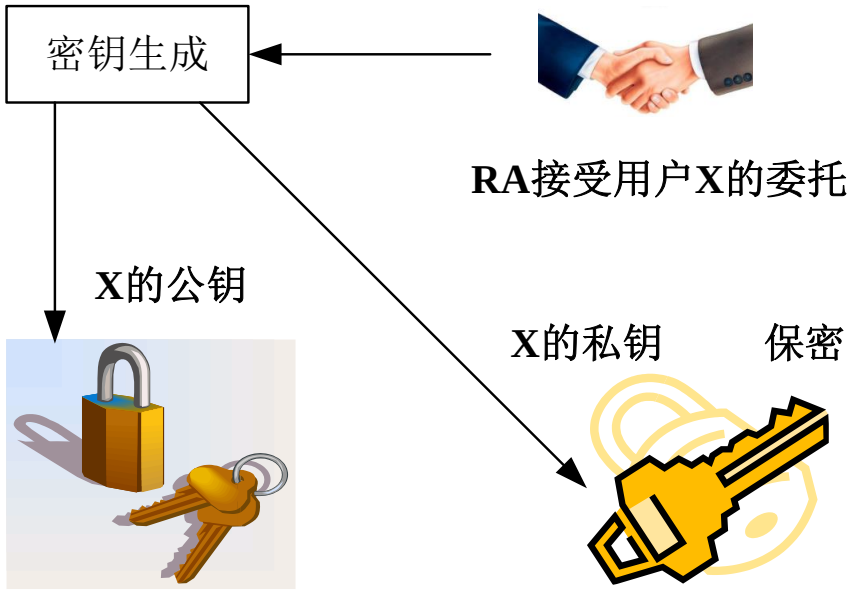


图8

注册机构主体生成密钥对示意图

第2步：注册。该步骤发生在第1步由主体生成密钥对情形下，若在第1步由RA为主体生成密钥对，则该步骤在第1步中完成。

- 假设用户生成密钥对，则要向注册机构发送公钥和相关注册信息(如主体名，将置于数字证书中)及相关证明材料。用户在特定软件的导引下正确地完成相应输入后通过Internet 提交至注册机构。
- **证书请求格式已经标准化，称为证书签名请求(CSR，Certificate Signing Request)**，PKCS#10证书申请结构如图9所示。有关CSR的详细信息可参看公钥加密标准PKCS#10。
- 注意：证明材料未必一定是计算机数据，有时也需纸质文档(如护照、营业执照、收入／税收报表复印件等)，如图10所示。

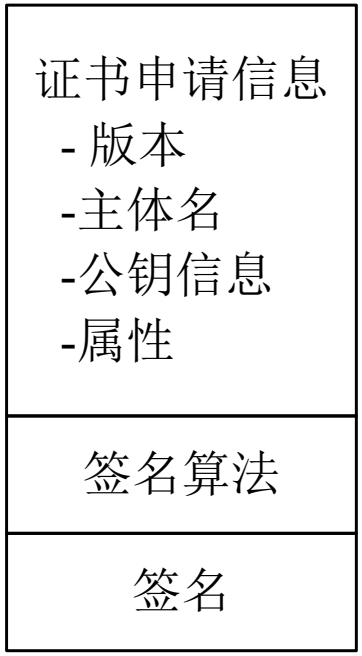


图9 PKCS#10证书申请结构

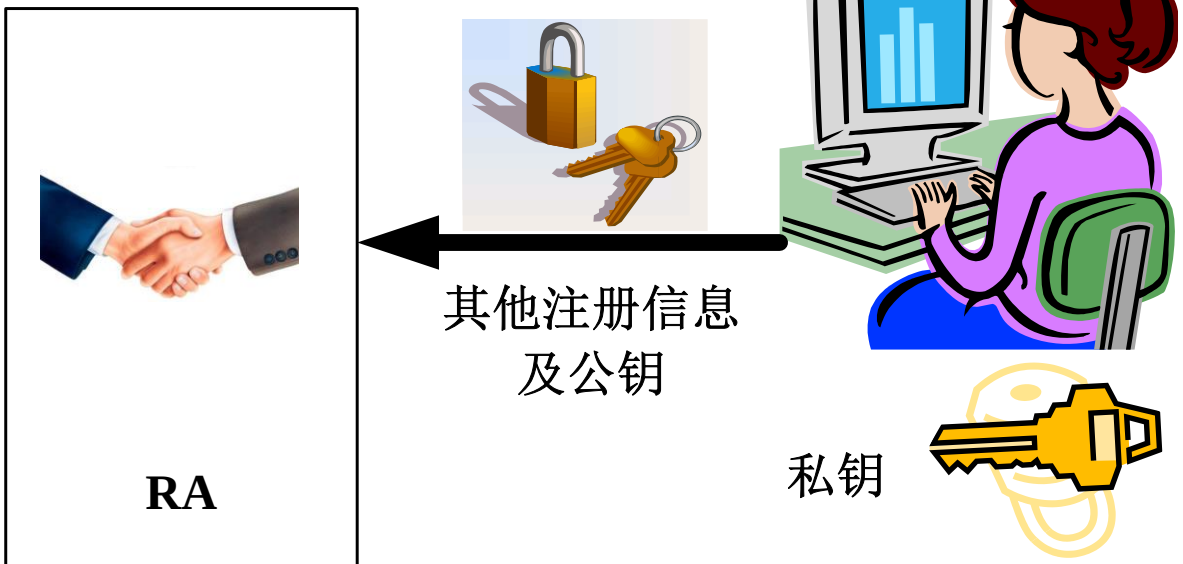


图10主体将公钥与证明材料发送的注册机构

第3步：验证。接收到公钥及相关证明材料后，注册机构须验证用户材料，验证分为以下两个层面。

(1)RA要验证用户材料，以明确是否接受用户注册。若用户是组织，则RA需要检查营业记录、历史文件和信用证明；若用户为个人，则只需简单证明，如验证邮政地址、电子邮件地址、电话号码或护照、驾照等。

(2)确保请求证书的用户拥有与向RA的证书请求中发送的公钥相对应的私钥。这个检查被称为检查私钥的拥有证明(POP，Proof Of Possession)。主要的验证方法有如下几种。

①RA可要求用户采用私钥对证书签名请求进行数字签名。若RA能用该用户公钥验证签名正确性，则可相信该用户拥有与其证书申请中公钥一致的私钥。

②RA可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，则可相信该用户拥有与公钥相匹配的私钥。

③RA可将CA所生成的数字证书采用用户公钥加密后，发送给该用户。用户需要用与公钥匹配的私钥解密方可取得明文证书——也实现了私钥拥有证明的验证。

第4步：证书生成

- 设上述所有步骤成功，则RA将用户的所有细节传递给证书机构。证书机构进行必要的验证，并生成数字证书。证书机构将证书发给用户，并在CA维护的证书目录(Certificate Directory)中保留一份证书记录。然后证书机构将证书发送给用户，可附在电子邮件中；也可向用户发送一个电子邮件，通知其证书已生成，让用户从CA站点下载。对于通用的编辑器而言，**数字证书的格式实际上是不可读的，但应用程序可对数字证书进行分析解释**，例如，打开 Internet Explorer 浏览器浏览证书时，可以看到可读格式的证书细节。

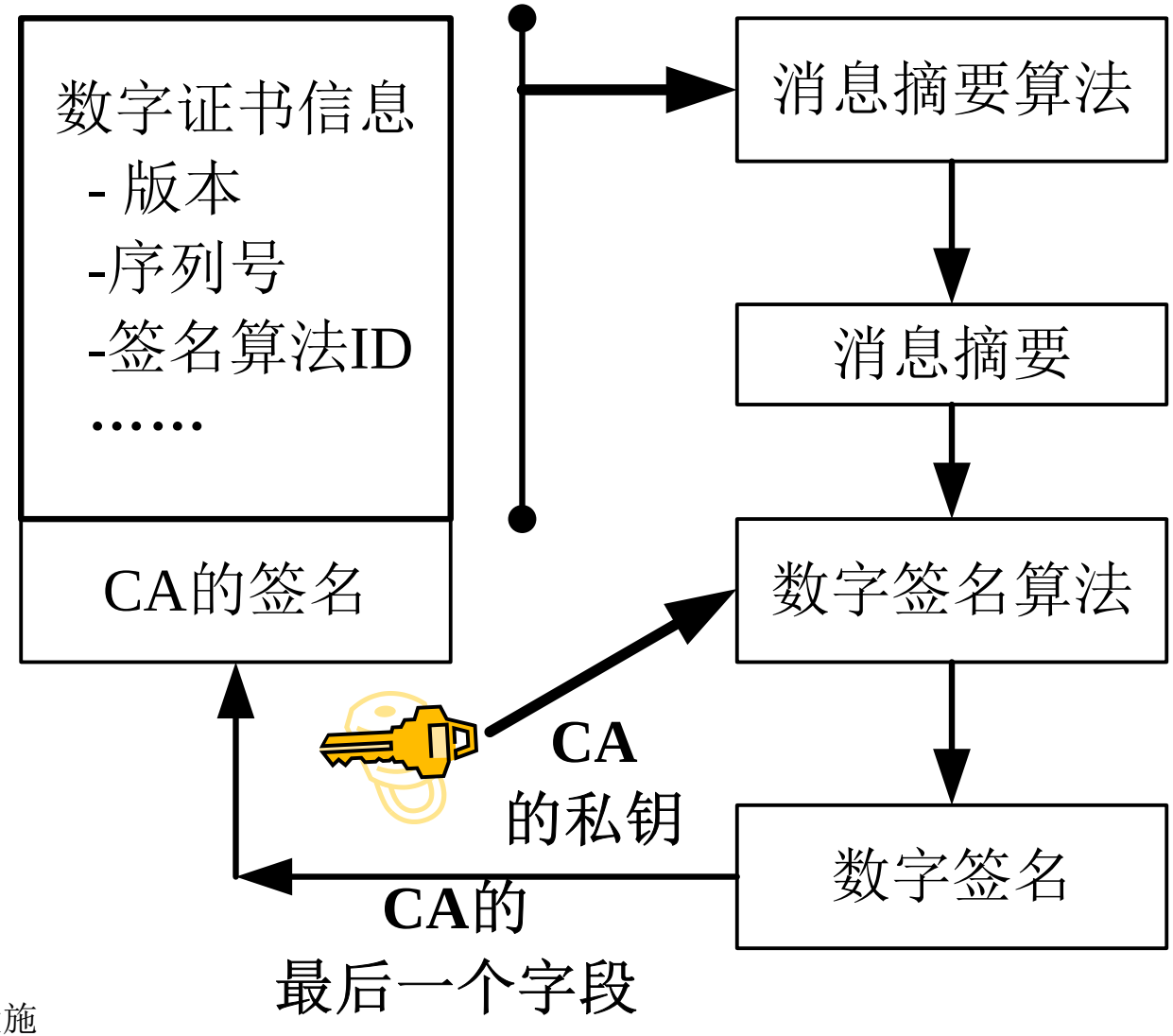
4.2.4 数字证书的签名与验证

- 正如护照需要权威机构的印章与签名一样，数字证书也需证书机构CA采用其私钥签名后方是有效、可信的。接下来，分别就CA签名证书及数字证书验证加以介绍。

1. CA签名证书

- 此前介绍过X.509证书结构，其中最后一个字段是证书机构的数字签名，即每个数字证书不仅包含用户信息(如主体名、公钥等)，同时还包含证书机构的数字签名。CA对数字证书签名过程如图11所示。

图11 CA对数字证书签名过程



- 由图11可知，在向用户签发数字证书前，CA首先要对证书的所有字段计算一个消息摘要(使用MD5或SHA1等杂凑算法)，而后用CA私钥加密消息摘要(如采用 RSA算法)，构成CA的数字签名。CA将计算出的数字签名作为数字证书的最后一个字段，类似于护照上的印章与签名。该过程由密码运算程序自动完成。

2.数字证书的验证

数字证书的验证步骤如图12所示。主要包括如下几步。

(1)用户将数字证书中除最后一个字段以外的所有字段输入消息摘要算法(杂凑算法)。该算法与CA签发证书时使用的杂凑算法相同，CA会在证书中指定签名算法及杂凑算法，令用户知道相应的算法信息。

(2)由消息摘要算法计算数字证书中除最后一个字段外其他字段的消息摘要，设该消息摘要为MD1。

(3)用户从证书中取出CA的数字签名(证书中最后一个字段)。

(4)用户用CA的公钥对CA的数字签名信息进行解密运算。

(5)解密运算后获得CA签名所使用的消息摘要，设为MD2。

(6)用户比较MD1与MD2。若两者相符，即MD1=MD2，则可肯定数字证书已由 CA用其私钥签名，否则用户不信任该证书，将其拒绝。

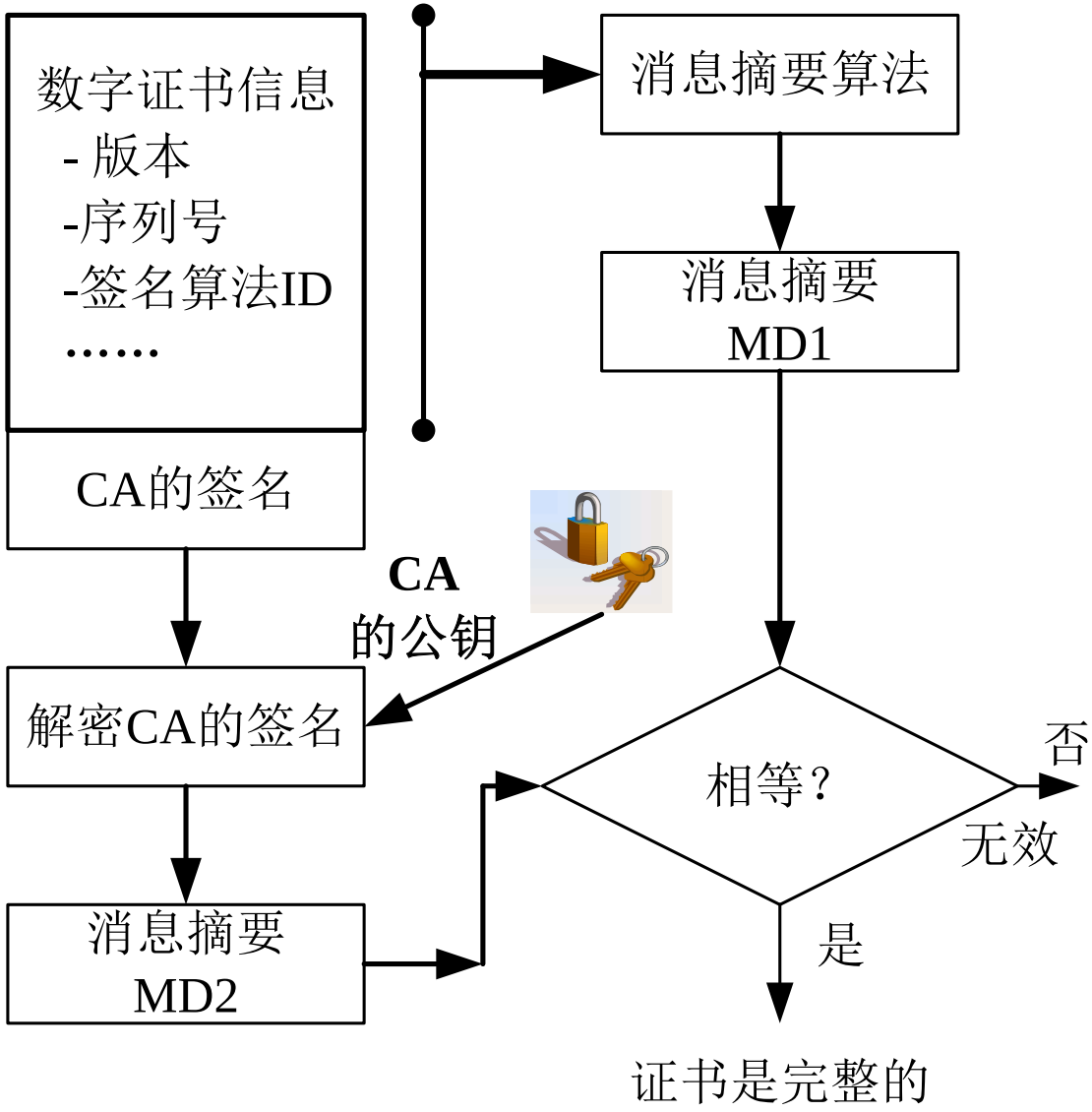

数字证书信息
- 版本
-序列号
-签名算法ID
……
消息摘要算法
消息摘要
MD1
CA的签名
CA
的公钥
解密CA的签名
消息摘要
MD2
相等？
否
无效
是
证书是完整的

图12

4.2.5 数字证书层次与自签名数字证书

- 设有两个用户Alice与Bob，希望进行安全通信，在Alice收到Bob的数字证书时，需对该证书进行验证。由前可知，验证证书时需使用颁发该证书的CA的公钥，这就涉及如何获取CA公钥的问题。
- 若Alice与Bob属于相同的证书机构(CA)，则Alice显然已知签发Bob证书的CA的公钥。若Alice与Bob归属于不同的证书机构，则Alice需通过如图13所示的**信任链**(CA**层次结构**)获取签发证书的CA公钥。

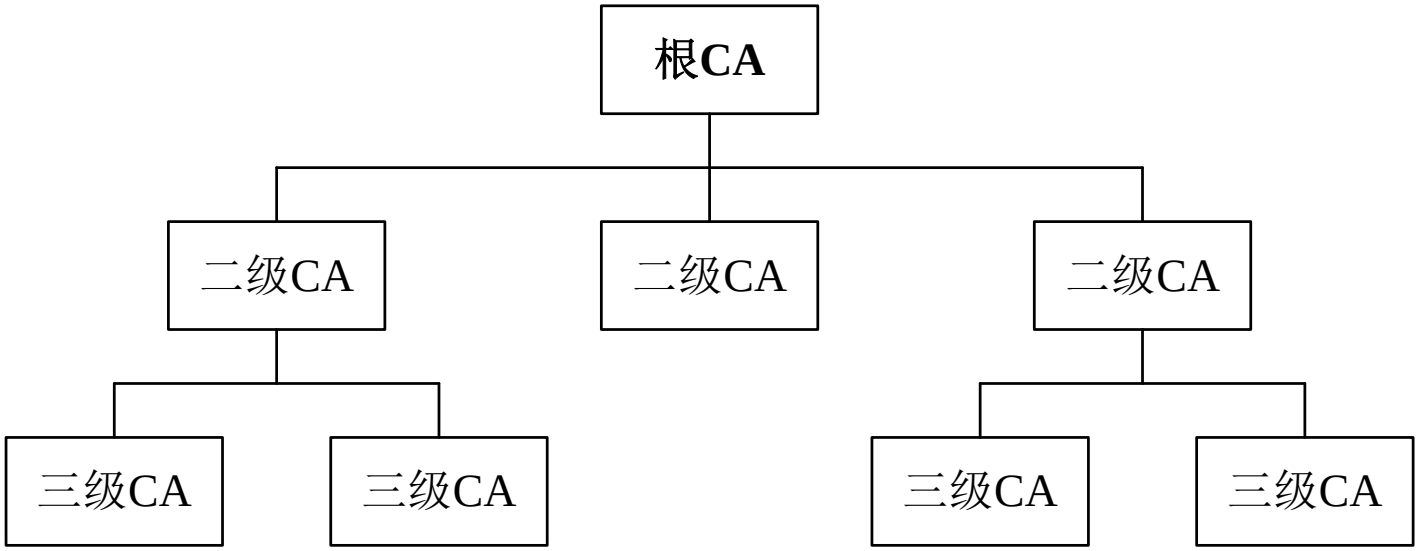
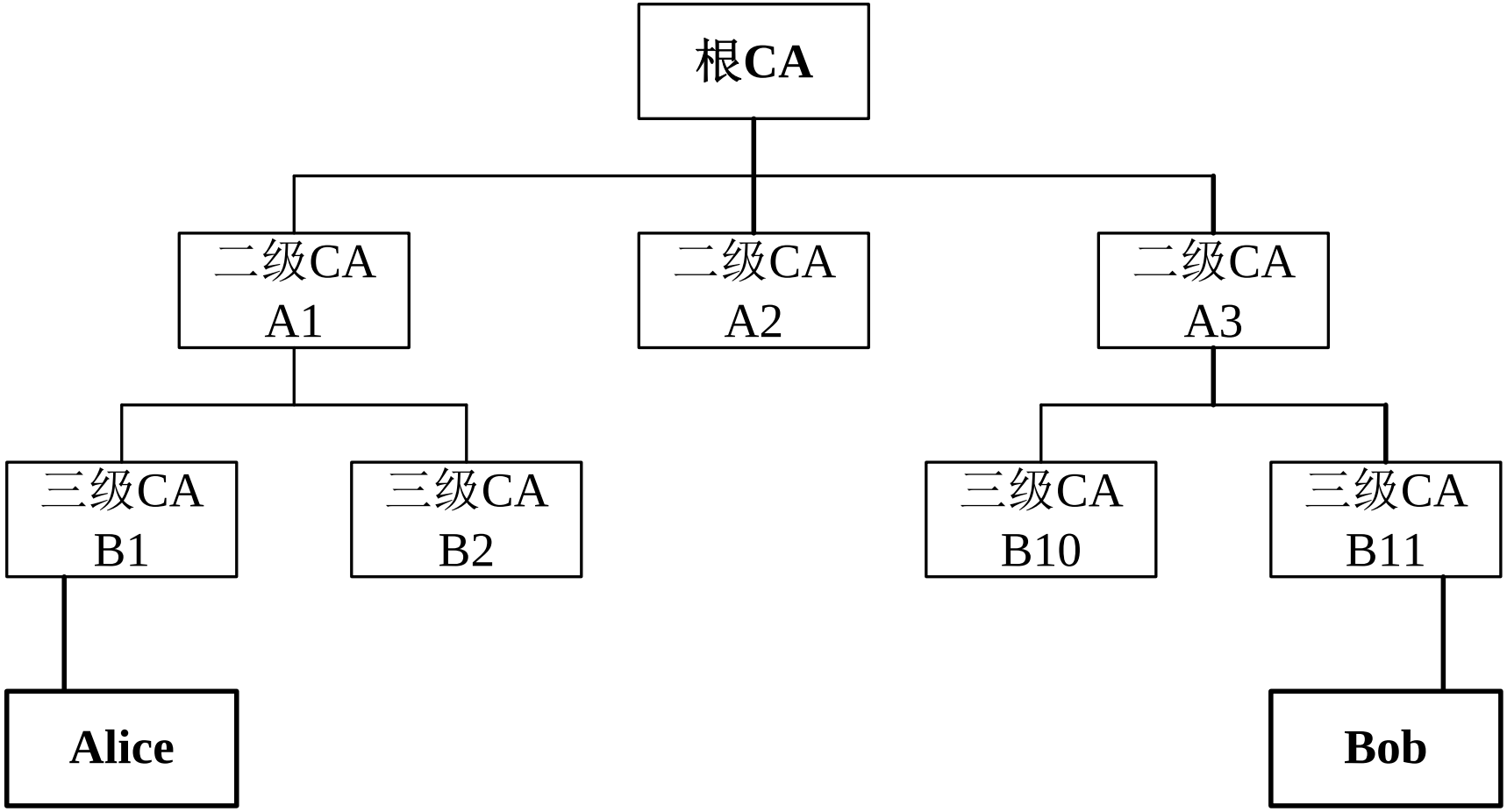


图13 信任链

- 由图13可看出，CA层次从根CA开始，根CA下面有一个或多个二级CA，每个二级CA下面有一个或多个三级CA，等等，类似于组织中的报告层次体系，CEO或总经理具有最高权威，高级经理向CEO或总经理报告，经理向高级经理报告，员工向经理报告……
- CA的层次结构使根CA不必管理所有的数字证书，可以将该任务委托给二级机构，每个二级CA又可在其区域内指定三级CA，每个三级CA又可指定四级CA，依次进行。
- 如图14所示，若Alice从三级CA(B1)取得证书，而Bob从另一个三级CA(B11)取得证书。显然，Alice不能直接获取B11的公钥，因此，除了自身证书外，Bob还需向 Alice发送其CA(B11)的证书，告知Alice B11的公钥。Alice根据B11的公钥对Bob证书进行计算验证。

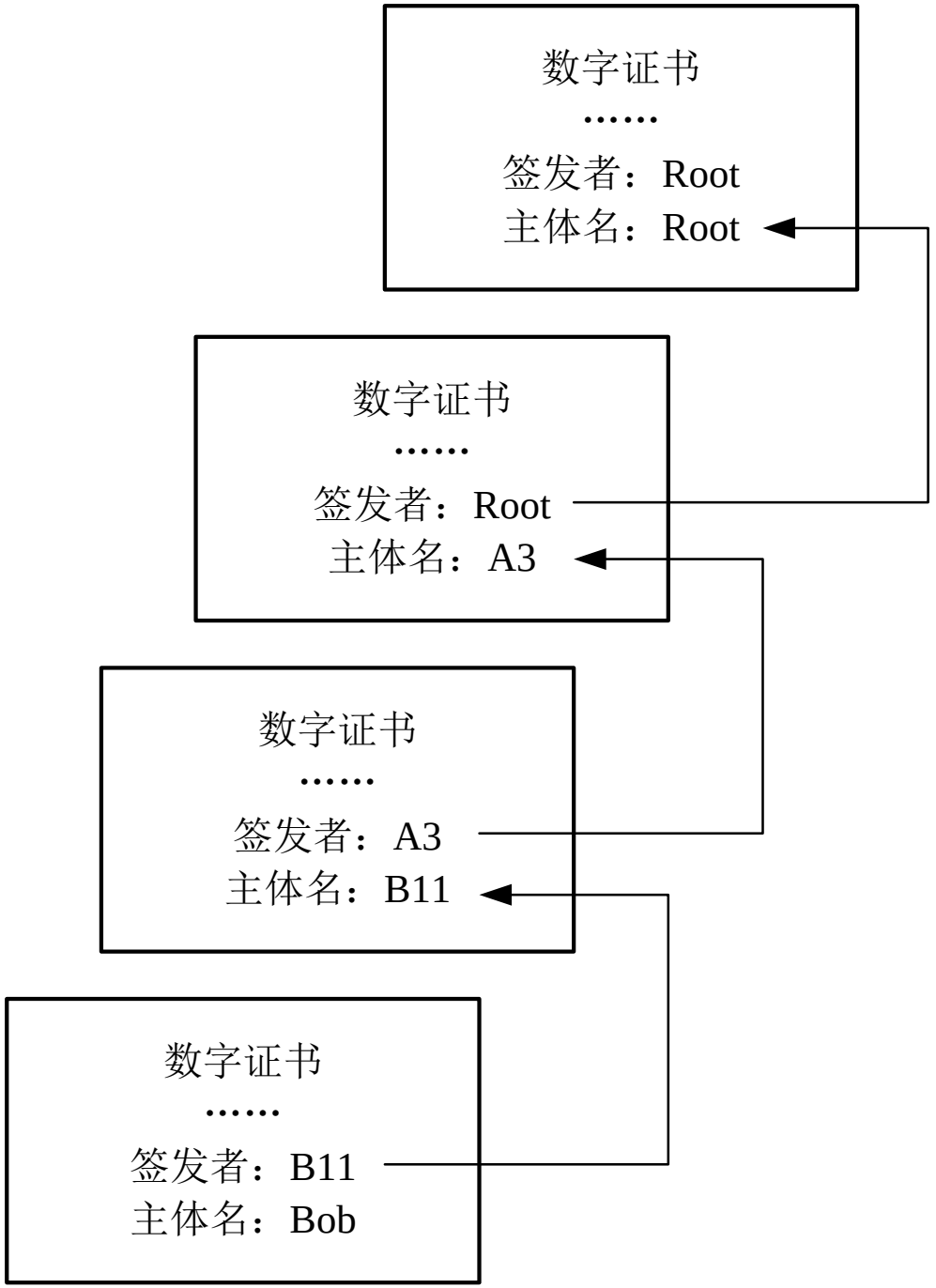
图14 同一根CA中不同CA所辖用户



- 显然，在使用B11公钥对Bob证书进行验证前，Alice需对B11证书的正确性进行验证(确认对B11证书的信任)。由图14可见，B11的证书是由A3签发的，则Alice需获得A3的公钥以验证A3对B11证书的签名。同理，为确保A3公钥的真实性与正确性，Alice需获取A3的证书，并需获得根CA公钥对A3证书进行验证。
- 证书层次与根 CA的验证问题如图15所示。

图15

- 证书层次与根CA的验证问题



- 由图15可见，根CA是验证链的最后一环，根CA自动作为可信任CA，**根CA证书为自签名证书**(Self-signed certificate)，**即根CA对自己的证书签名**，如图16所示，证书的签发者名和主体名均指向根CA。**存储与验证证书的软件中包含预编程、硬编码的根CA证书。**

数字证书

……

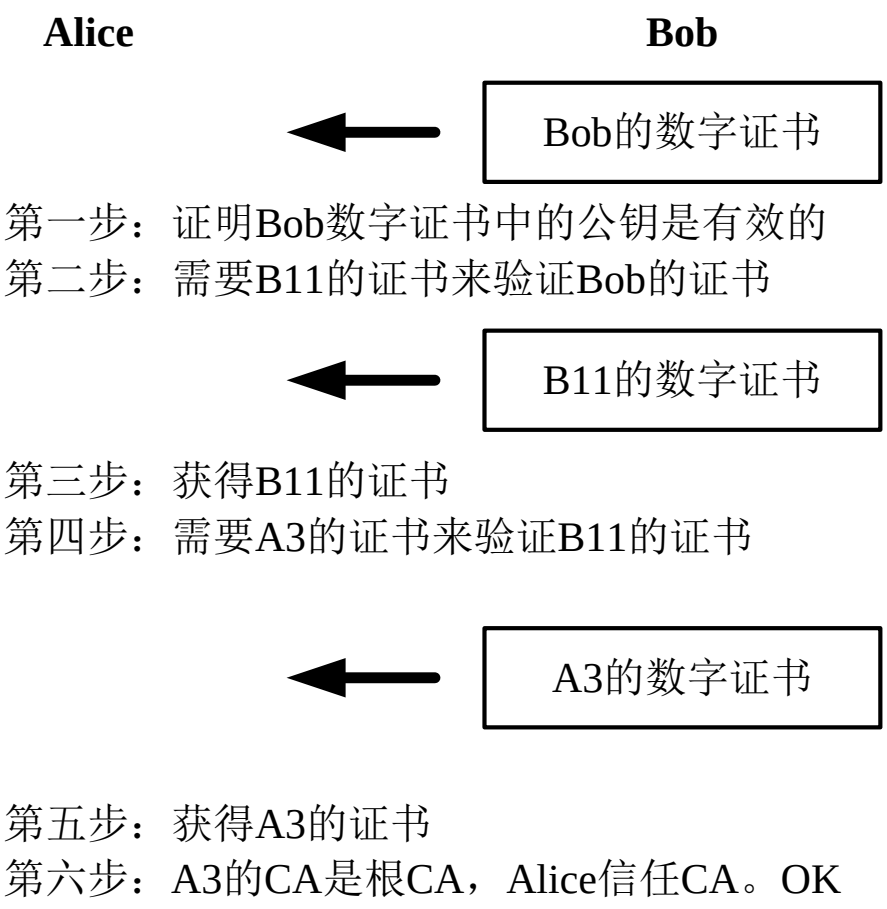
签发者：Root

主体名：Root

图16 自签名证书

图17 验证证书链的过程

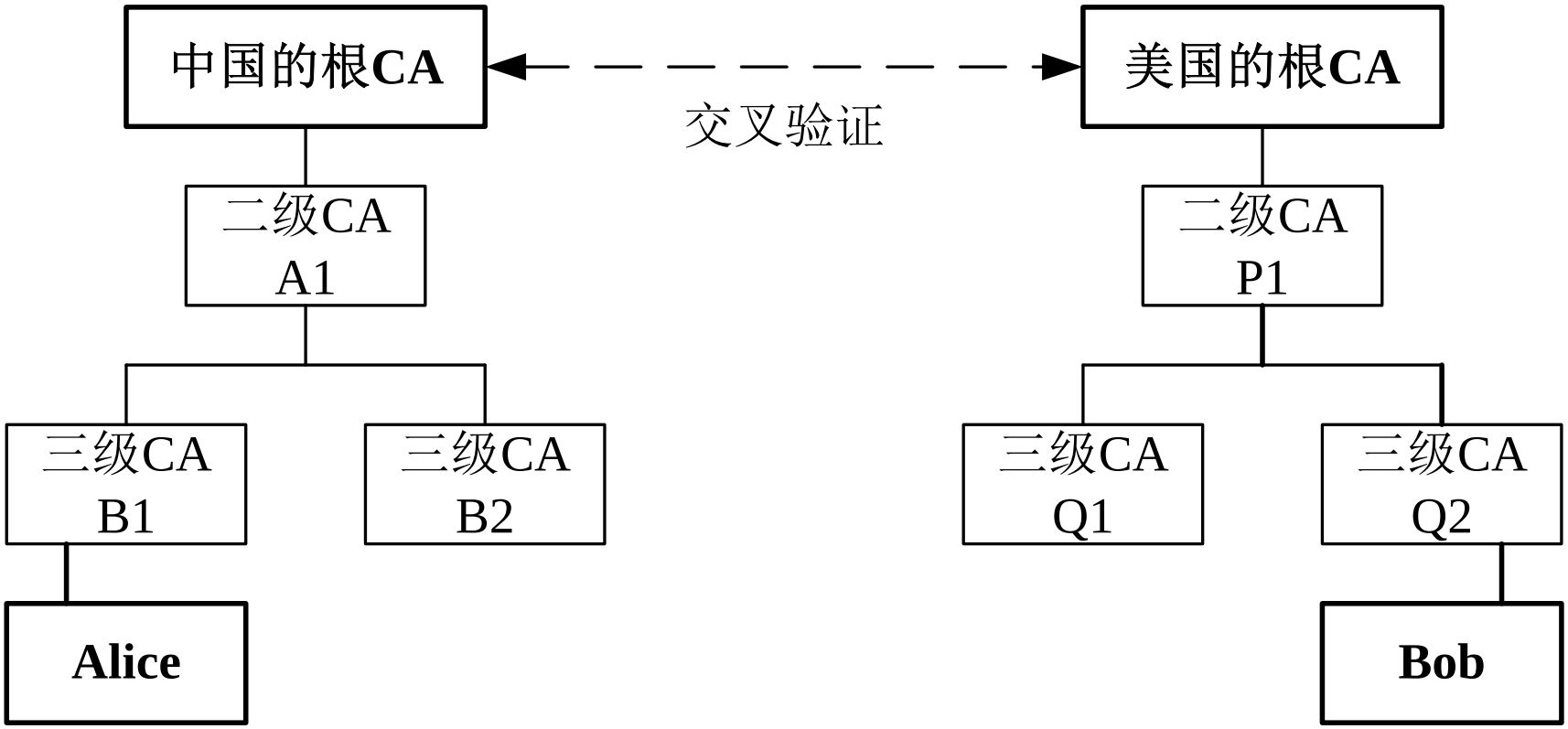
- 由于**根CA证书存放于Web浏览器和Web服务器之类基础软件中**，因此Alice无须担心根CA证书认证问题，**除非其使用的基础软件本身来自于非信任站点**。Alice只需采用遵循行业标准、被广泛接受的应用程序，即可保证根CA证书的有效性。
- 图17显示了验证证书链的过程。



4.2.6 交叉证书

- 每个国家均拥有不同的根CA，即使同一国家也可能拥有多个根CA。例如，美国的根 CA有Verisign、Thawte和美国邮政局。这时，不是各方都能信任同一个根CA。若Alice与Bob身处不同国家，即根CA不同时，也存在着**根CA的信任问题**。
- 针对以上情形，采用**交叉证书(Cross—Certification)**。由于实际中不可能有一个认证每个用户的统一CA，因此要用分布式CA认证各个国家、政治组织与公司机构的证书。这种方式减少了单个CA的服务对象，同时确保CA可独立运作。此外，交叉证书使不同PKI域的CA和最终用户可以互动。交叉证书是对等CA签发，建立的是非层次信任路径。

图18 CA的交叉证书


中国的根CA
美国的根CA
交叉验证
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

- 如图18所示，Alice与Bob的根CA不同，但他们可进行交叉认证，即Alice的根 CA从Bob的根CA那里取得了自身的证书，同样Bob的根CA从Alice的根CA处取得了自己的证书。
- 尽管Alice的基础软件只信任其自己的根CA，但因为Bob的根CA得到了Alice的根CA的认证，则Alice也可信任Bob的根CA。Alice可采用下列路径验证 Bob的证书：Bob-Q2-P1-Bob’s RCA-Alice’s RCA。
- 利用证书层次、自签名证书和交叉证书技术，令所有用户均可验证其他用户的数字证书，以确定信任证书或拒绝证书。

4.2.7 数字证书的撤销

- 数字证书撤销的常见原因有：
  - ①数字证书持有者报告该证书中指定公钥对应的私钥被破解(被盗)；
  - ②CA发现签发数字证书时出错；
  - ③证书持有者离职，而证书为其在职期间签发的。
- 发生第一种情形需由证书持有者进行证书撤销申请；发生第三种情形时需由组织提出证书撤销申请；发生第二种情形时，CA启动证书撤销。CA在接到证书撤销请求后，首先认证证书撤销请求，然后方接受请求，启动证书撤销，以防止攻击者滥用证书撤销过程撤销他人证书。

图19 证书撤销状态检查机制

Alice使用Bob的证书与Bob安全通信前，需明确以下两点：

(1)该证书是否属于Bob?

(2)该证书是否有效，是否被撤销?

- Alice可通过证书链明确第一个问题，而明确第二个问题则需采用证书撤销状态检查机制。CA提供的证书撤销状态检查机制如图19所示。

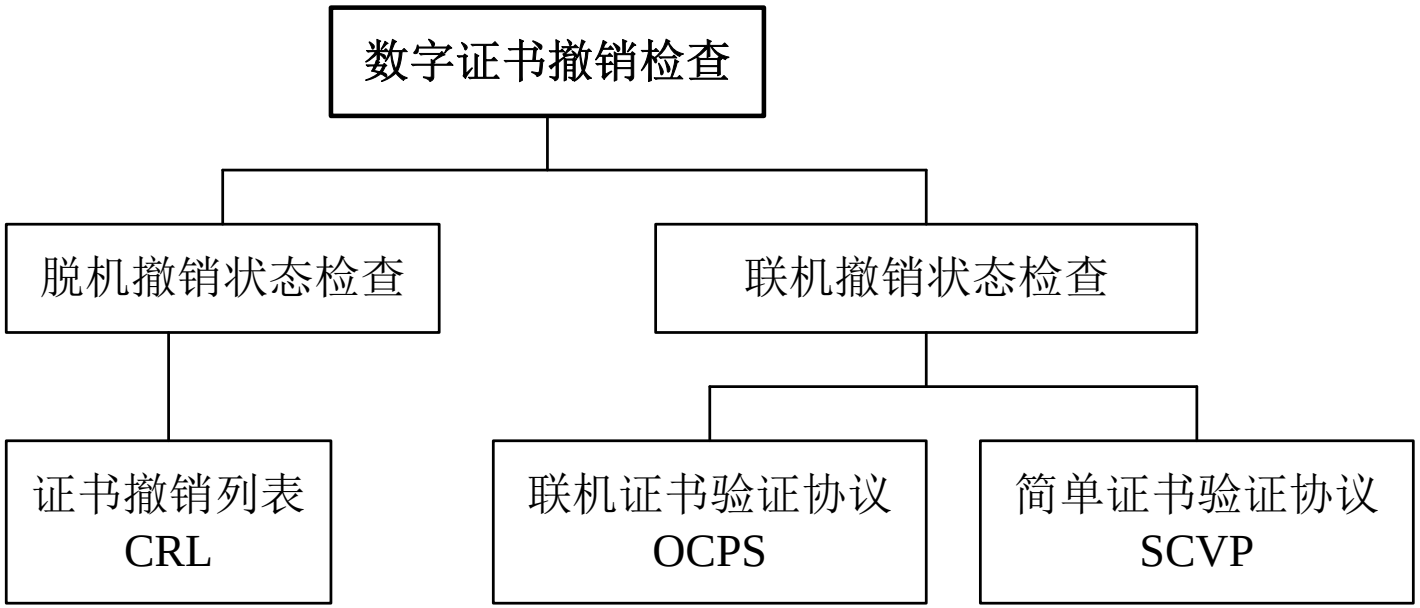


图19

下面对这几种撤销检查机制逐一加以介绍。

1.脱机证书撤销状态检查

- **证书撤销列表**(CRL，Certificate Revocation List)**是脱机证书撤销状态检查的主要方法**。最简单的CRL是由CA定期发布的证书列表，标识该CA撤销的所有证书。但该表中不包含过了有效期的失效证书。**CRL中只列出在有效期内因故被撤销的证书。**
- 每个CA签发自己的CRL，CRL包含相应的CA签名，易于验证。CRL为一个依时间增长的顺序文件，包括在有效期内因故被撤销的所有证书，是CA签发的所有CRL的子集。每个CRL项目列出证书序号、撤销日期和时间、撤销原因。CRL顶层还包括CRL发布的日期、时间和下一个CRL发布时间。图20给出了CRL文件的逻辑视图。

图20 CRL文件的逻辑视图

CA: ABC Certificate Revocation List(CRL) This CRL: 1 Jan 2013, 10:00 am Next CRL: 12 Jan 2013, 10:00 am		
Serial Number	Date	Reason
1230001	30-Dec-12	Private key compromised
1350001	30-Dec-12	Changed job
……	……	……

Alice对Bob数字证书的安全性检查操作如下。

(1)证书有效期检查：比较当前日期与证书有效期，确保证书在有效期内。

(2)签名检查：检查Bob的证书能否用其CA的签名验证。

(3)证书撤销状态检查：根据Bob的CA签发的最新CRL检查Bob的证书是否在证书撤销列表中。

完成以上检查后，Alice方能信任Bob的数字证书，相应过程如图21所示。

图21

Version	
Serial Number	检查3：必须保证该序列号不在CA的证书撤销列表CRL中
Signature Algorithm Identifier	
Issuer Name	
Validity Period	检查1：保证证书未过期
Subject Name	
Subject Public Key Information	
Issuer Unique ID	
Subject Unique ID	
Extensions	
Certification Authority’s Digital Signature	检查2：该证书必须能通过信任链进行验证

- 随着时间的推移，CRL可能会变得很大。一般假设，每年撤销的未到期证书达10％左右，若CA有100 000用户，则两年时间可能在CRL中有20 000个项目，数目是相当庞大的。在这种情形下，通过网络接收CRL文件将是一个很大的瓶颈。为解决该问题，引出了**差异CRL(Delta CRL)**的概念。
- 最初，CA可以向使用CRL服务的用户发一个一次性的完全更新CRL，称为基础CRL(Base CRL)。下次更新时，CA不必发送整个CRL，而只需发送上次更新以来改变的CRL。这个机制令CRL文件的长度缩小，从而加快传输速度。基础CRL的改变称为差异CRL，差异CRL也是一个需CA签名的文件。图22给出了每次签发完整CRL与只签发差异CRL的区别。

图22 每次签发完整CRL与签发差异CRL的区别

Frist CRL distribution	CA: ABC CRL ……		CA: ABC Base CRL ……
CRL Update 1	CA: ABC CRL ……		CA: ABC Delta CRL ……
CRL Update 2	CA: ABC CRL ……		CA: ABC Delta CRL ……
	方法1：每次签发完整的CRL		方法2：只签发差异CRL

使用CRL时，需注意以下几点：

①差异CRL文件包含一个差异CRL指识符，告知用户该CRL为差异CRL，用户需将该差异CRL文件与基础CRL文件一起使用，得到完整CRL；

②每个CRL均有序号，用户可检查是否拥有全部差异CRL；

③基础CRL可能有一个差异信息指识符，告知用户这个基础CRL具有相应的差异CRL，还可提供差异CRL地址和下一个差异CRL的发布时间。图23给出了CRL的标准格式。

图23 CRL的标准格式

<table>
<tr><td colspan="3">Version
Signature Algorithm Identifier
Issuer Name
This Update(Date and Time)
Next Update(Date and Time)</td><td>头字段</td></tr>
<tr><td>Serial Number</td><td>Date</td><td>Reason</td><td rowspan="4">重复项</td></tr>
<tr><td>1230001</td><td>30-Dec-12</td><td>Private key compromised</td></tr>
<tr><td>1350001</td><td>30-Dec-12</td><td>Changed job</td></tr>
<tr><td>……</td><td>……</td><td>……</td></tr>
<tr><td colspan="3">CRL Extension</td><td rowspan="2">尾字段</td></tr>
<tr><td colspan="3">Signature</td></tr>
</table>

- 如图23所示，CRL格式中有几个头字段、几个重复项目和几个尾字段。显然，序号、撤销日期、CRL项目扩展之类的字段要对CRL中的每个撤销证书重复。而其他字段构成头字段、尾字段两部分。下面介绍这些字段，如表3所示。

表3 CRL的不同字段

字段	描述
版本(Version)	CRL版本
签名算法标识符 Signature Algorithm Identifier	CA签名CRL所用的算法 (如SHA-1和RSA)
签发者名(Issuer Name)	CA的可区分名(DN)
本次更新日期与时间 This Update Date and Time	签发这个CRL的日期与时间
下次更新日期与时间 Next Update Date and Time	签发下一个CRL的日期与时间
用户证书序号 User Certificate Serial Number	被撤销证书的序号
撤销日期(Revocation Date)	证书的撤销日期和时间
CRL项目扩展(CRL Entry Extension)	每个CRL项目有一个扩展
CRL扩展(CRL Extension)	每个CRL有一个扩展
签名(Signature)	CA对该CRL的签名

表4 CRL项目扩展

- 这里，需明确区别CRL项目扩展与CRL扩展，CRL项目扩展对每个撤销证书重复，而整个CRL只有一个CRL扩展，详见表4和表5。

表4

字段	描述
原因代码(Reason Code)	指定证书撤销原因，可能是Unspecified, Key Compromise, CA Compromise, Superseded, Certificate Hold
扣证指示代码 Hold Instruction Code	证书可以暂扣，即在指定时间内失效，该字段指定扣证原因
证书签发者 Certificate Issuers	标识证书签发者名和间接CRL。间接CRL是第三方提供的，而非证书签发者提供。第三方可以汇总多个CA的CRL为一个合并的CRL，以方便使用
失效日期 Invalidity Date	失效日期

表5 CRL扩展

字段	描述
机构密钥标识符 (Authority Key Identifier)	区别一个CA使用的多个CRL签名密钥
签发者别名(Issuer Alternative Name)	签发者的一个或多个别名
CRL号(CRL Number)	序号(随每个CRL递增)
差异CRL标识符(Delta CRL Indicator)	表示CRL为差异CRL
签发发布点 (Issuing Distribution Point)	表示CRL发布点或CRL分区

- 和最终用户一样，CA本身也用证书标识。在某些情形下，CA证书也需撤销，类似于 CRL提供最终用户证书的撤销信息表，机构撤销列表(ARL)提供了CA证书的撤销信息表。

2.联机证书撤销状态检查

- 由于CRL可能过期，同时CRL存在长度问题，基于CRL的脱机证书撤销状态检查不是检查证书撤销的最好方式。因此，出现了两个联机检查证书状态协议：**联机证书状态协议和简单证书检验协议**。
- **联机证书状态协议**(OCSP，Online Certificate Status Protocol)**可以检查特定时刻某个数字证书是否有效，是联机检查方式。**联机证书状态协议令证书检验者可以实时检查证书状态，从而提供了更简单、快捷、有效的数字证书验证机制。与CRL不同，该方式无须下载证书列表。下面介绍联机证书状态协议的工作步骤。

(1)CA提供一个服务器，称为OCSP响应器(OCSP Responder)，该服务器包含最新证书撤销信息。请求者(客户机)发送联机证书状态查询请求(OCSP Request)，检查该证书是否撤销。OCSP最常用的基础协议是HTTP，但也可以使用其他应用层协议(如 SMTP)，如图24所示。实际上，OSCP请求还包括OSCP协议版本、请求服务和一个或几个证书标识符(其中包含签发者的消息摘要、签发者公钥的消息摘要和证书序号)。为简单起见，暂忽略这些细节。

图24 OCSP请求

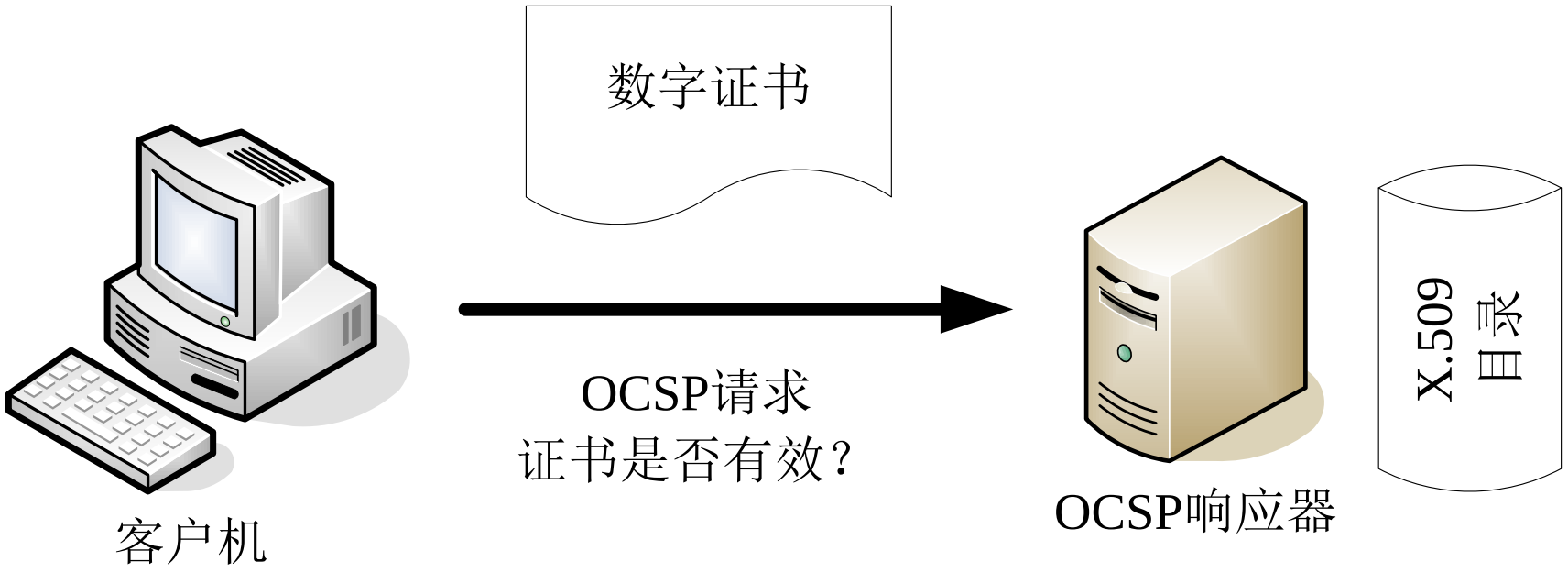
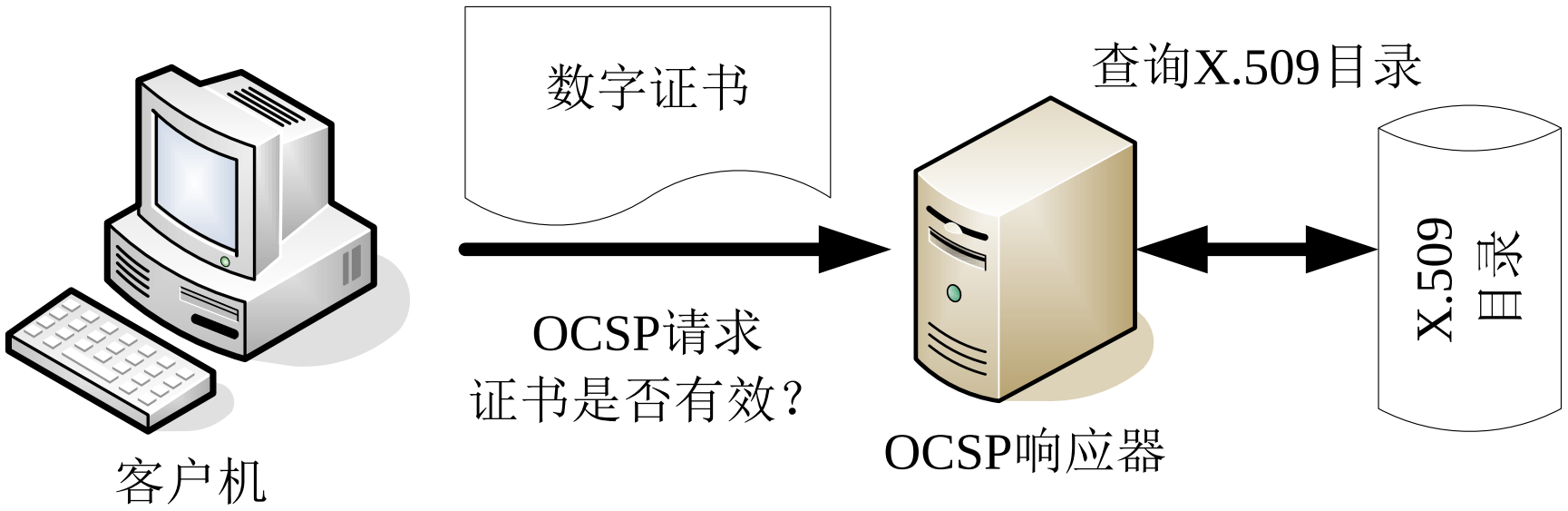


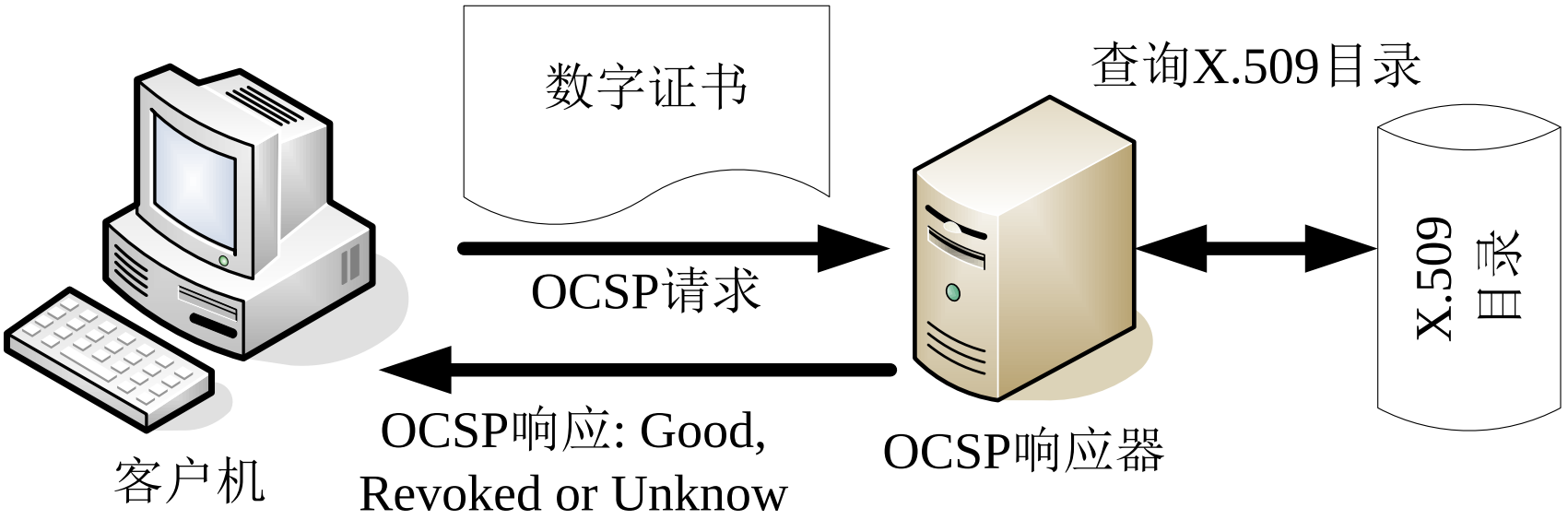
图25 OCSP证书撤销状态检查

(2)OCSP响应器查询服务器的X.500目录(CA不断向其提供最新证书撤销信息)，以明确特定证书是否有效，如图25所示。



(3)根据X.500目录查找的状态检查结构，OCSP响应器向客户机发送数字签名的 OCSP响应(OCSP Response)，原请求中的每个证书有一个OCSP响应。OCSP响应可以取3个值，即Good、Revoked或Unknown。OCSP响应还可以包含撤销日期、时间和原因。客户机要确定相应的操作。一般而言，建议只在OCSP响应状态为Good时才认为证书有效，OCSP响应如图26所示。

图26 OCSP响应


数字证书
查询X.509目录
OCSP请求
X.509目录
OCSP响应: Good,
Revoked or Unknow
客户机
OCSP响应器

- 需要注意的是，OCSP缺少对与当前证书相关的证书链有效性的检查。例如，假设 Alice要用OCSP验证Bob的证书，则OCSP只是告诉Alice，Bob的证书是否有效，而不检验签发Bob证书的CA的证书或证书链中更高层的证书。这些逻辑(验证证书链有效性)要放在使用OCSP的客户机应用程序中。另外，客户机应用程序还要检查证书有效期、密钥使用合法性和其他限制。
- **简单证书检验协议**(SCVP，Simple Certificate Validation Protocol)**目前还是草案**，是联机证书状态报告协议，用于克服OCSP的缺点。SCVP与OCSP在概念上非常相似，这里仅指出两者的差别，如表6所示。

表6 OCSP与SCVP的差别

特点	OCSP	SCVP
客户端请求	客户机只向服务器发送证书序号	客户机向服务器发送整个证书，因此服务器可以进行更多的检查
信任链	只检查指定证书	客户机可以提供中间证书集合，让服务器检查
检查	只检查证书是否撤销	客户机可以请求其他检查、考虑撤销类型，等等
返回信息	只返回证书状态	客户机可以指定感兴趣的其他信息
其他特性	无	客户机可以请求检查证书的过去事件。

4.2.8 漫游证书

- 数字证书应用的普及产生了证书的便携性需求。此前提供证书及其对应私钥移动性的实际解决方案主要分为两种：①智能卡技术，在该技术中，公钥 / 私钥对存放在卡上，但这种方法存在缺陷，如易丢失和损坏，并且依赖读卡器(虽然带USB接口的智能钥匙不依赖于读卡器，但成本太高)；②将证书和私钥复制到一张软盘上备用，但软盘不仅容易丢失和损坏，而且安全性较差。
- 一个新的解决方案就是使用漫游证书。它通过第三方软件提供，在任何系统中，只需正确配置，该软件(或插件)就可以允许用户访问自己的公钥 / 私钥对。其基本原理非常简单，如下所述。

(1)将用户的证书和私钥放在一个安全的中央服务器(称为**证件服务器**)数据库中，如图27所示。

图27 漫游证书用户注册

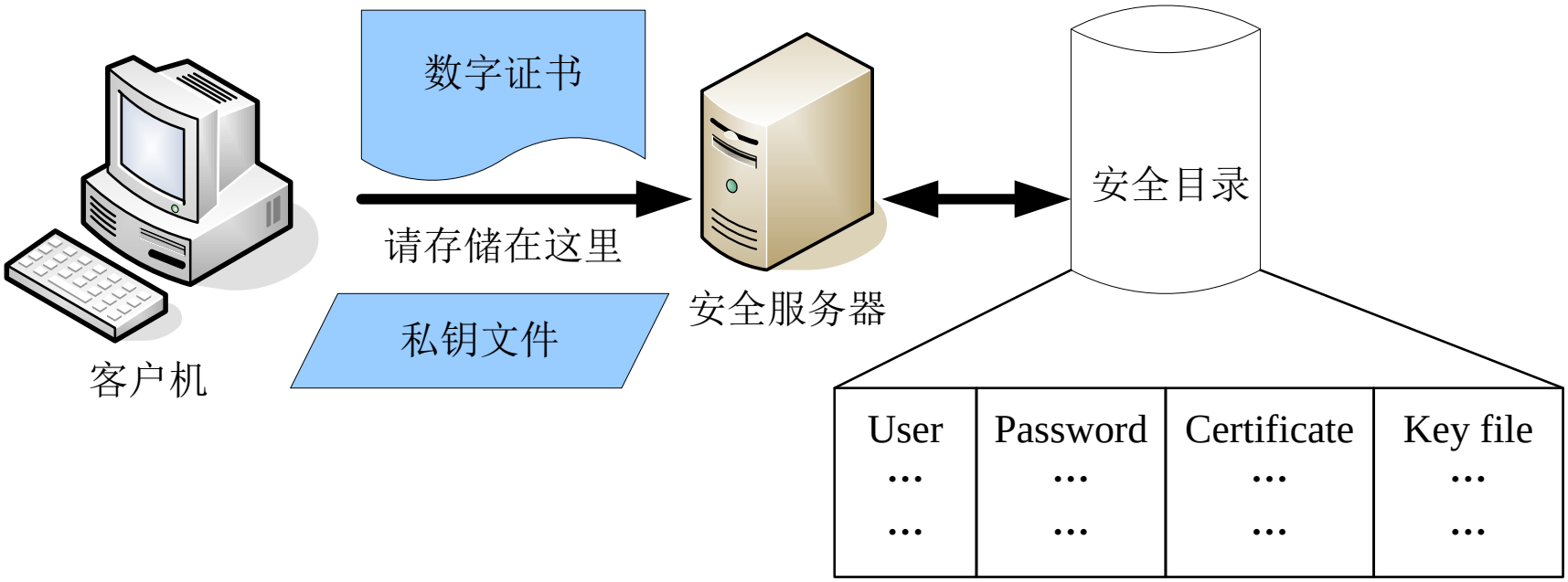


图28 漫游证书用户登录

(2)当用户登录到一个本地系统时，使用用户名和口令通过Internet向证件服务器认证自己，如图28所示。

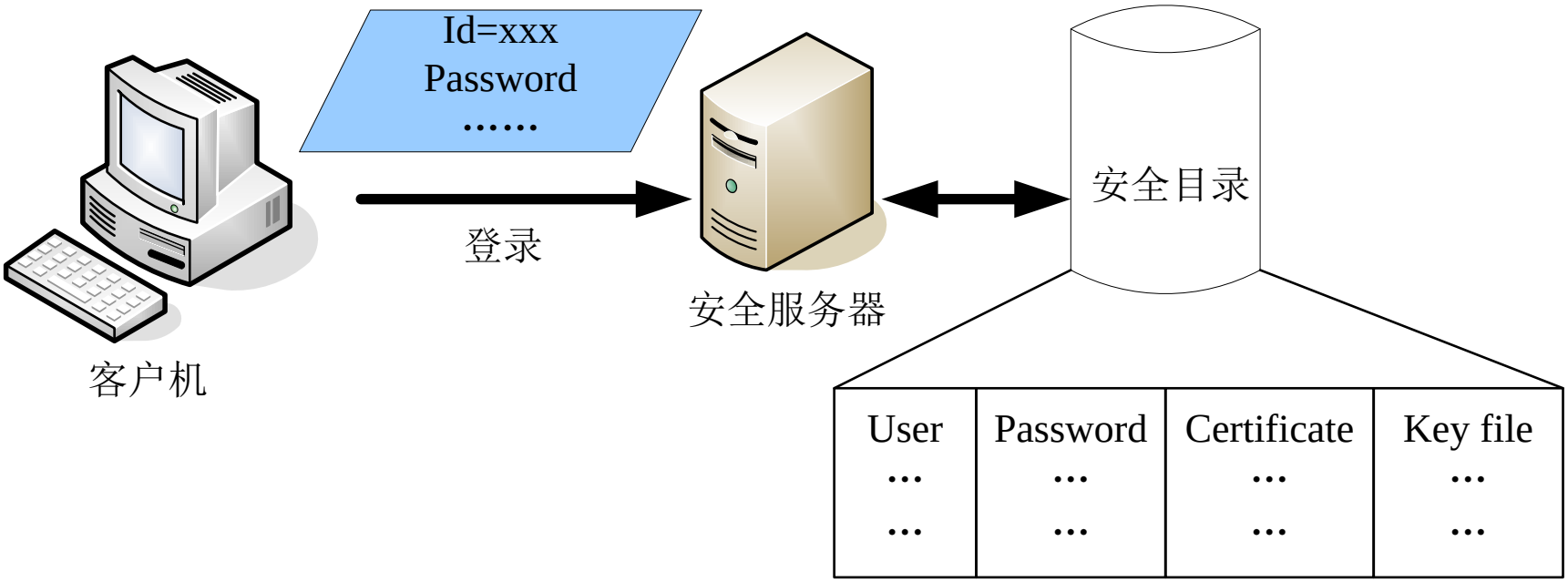
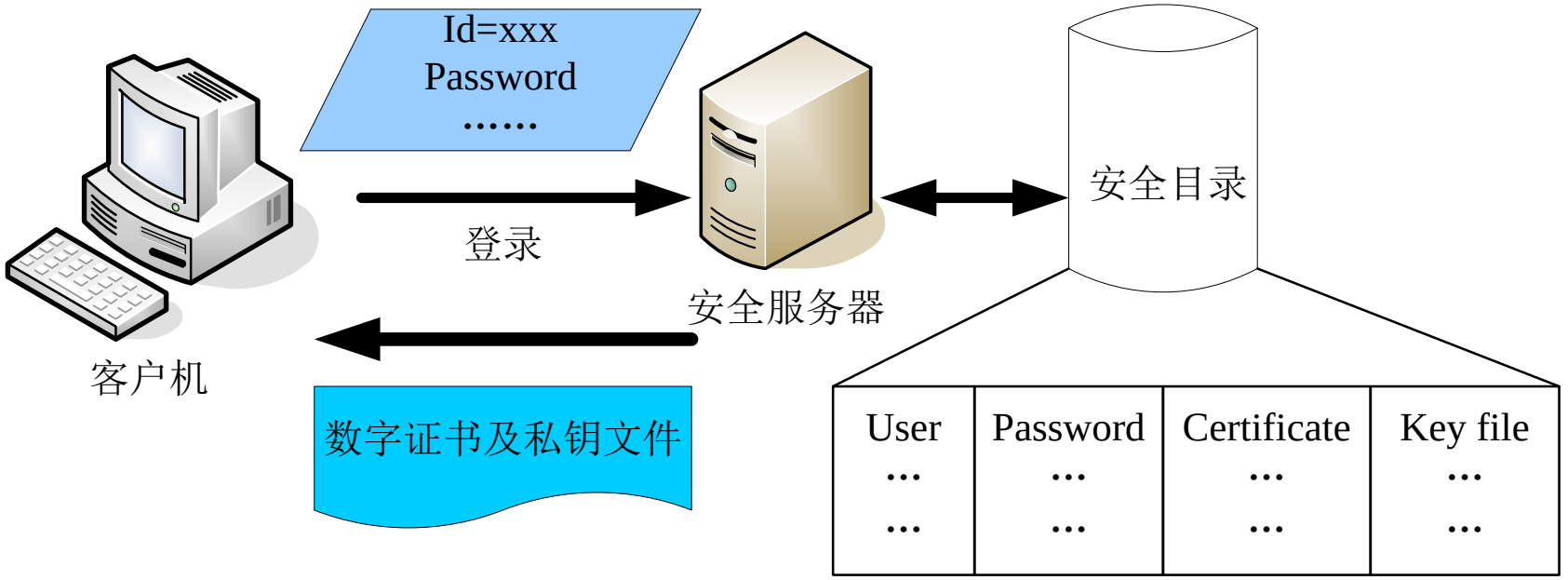


图29 漫游证书用户接收数字证书与私钥文件

(3)证件服务器用证件数据库验证用户名和口令，如果认证成功，则证件服务器将数字证书与私钥文件发送给用户，如图29所示。



(4)当用户完成工作并从本地系统注销后，该软件**自动删除存放在本地系统中的用户证书和私钥**。

- 这种解决方案的优点是可以明显提高易用性、降低证书的使用成本，但它与已有的一些标准不一致，因而在应用中受到了一定限制。在小额支付等低安全要求的环境中，该解决方案是一种较合适的方法。

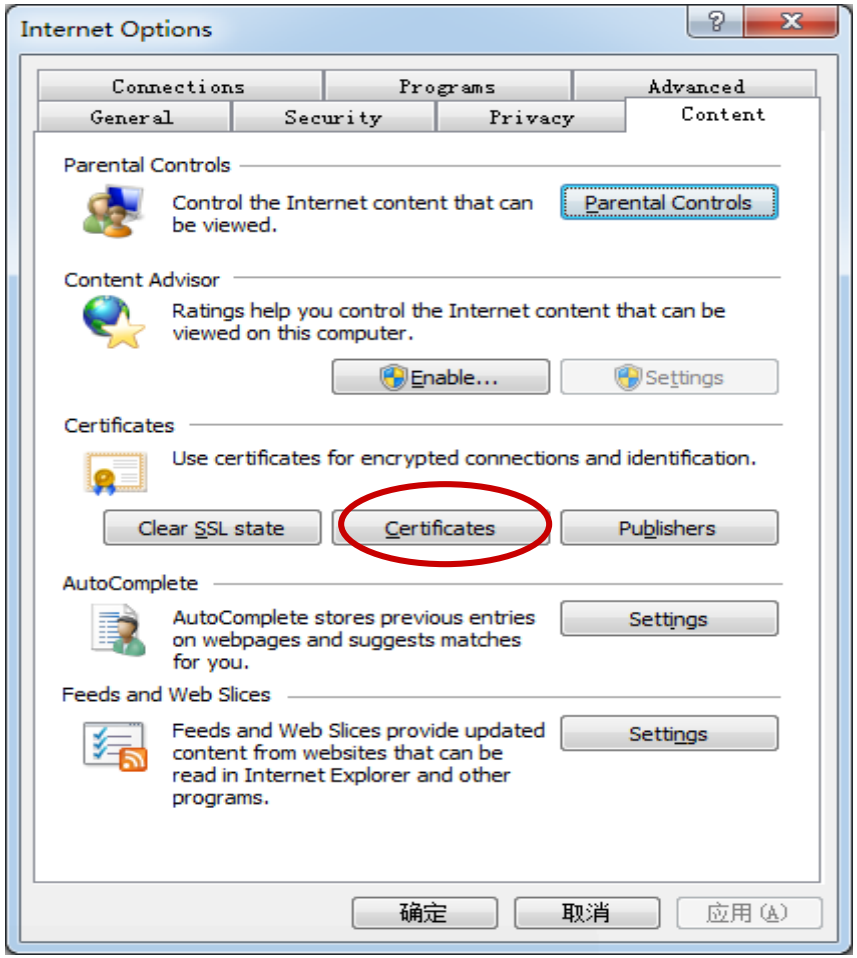
如何查看系统中的数字证书？

- iexplore中查看证书
- 环境：Windows7

演示

Linux下查看x.509证书

– gcr-viewer testCCB.cer



4.3 PKI体系结构——PKIX模型

- X.509标准定义了数字证书结构、格式与字段，还指定了发布公钥的过程。为了扩展该标准，令其更通用，Internet工作任务组(IETF)建立了**公钥基础设施**X.509(PKIX，Public Key Infrastructure X.509)工作组，扩展X.509标准的基本思想，指定在Internet中如何部署数字证书。此外，还为不同领域的应用程序定义了其他PKI模型。

- 本节仅对PKIX模型进行简要介绍。

4.3.1 PKIX服务

PKIX提供的公钥基础设施服务包括以下几个方面。

(1)注册：该过程是最终实体(主体)向CA介绍自己的过程，通常通过注册机构进行。

(2)初始化：处理基础问题，如最终实体如何保证对方是正确的CA。

(3)认证：CA对最终实体生成数字证书并将其交给最终实体，维护复制记录，并在必要时将其复制到公共目录中。

(4)密钥对恢复：一定时间内可能要恢复加密运算所用的密钥，以便旧文档解密。密钥存档和恢复服务可以由CA提供，也可由独立的密钥恢复系统提供。

(5)密钥生成： PKIX指定最终实体应能生成公钥/私钥对，或由CA/RA为最终实体生成(并将其安全地发布给最终实体)。

(6)密钥更新： 可以从旧密钥对向新密钥对顺利过渡，进行数字证书自动刷新。也可提供手工数字证书更新请求与响应。

(7)交叉证书： 建立信任模型，使不同CA认证的最终实体可以相互验证。

(8)撤销： PKIX可以支持两种证书状态检查模型——联机(使用OCSP)或脱机(CRL)

4.3.2 PKIX体系结构

- PKIX建立了综合性文档，介绍其体系结构模型的5个域，包括以下几方面。

(1) X.509 v3证书与v2证书撤销列表配置文件： X.509标准可以用各种选项描述数字证书扩展。PKIX把适合Internet 用户使用的所有选项组织起来，称为Internet用户的配置文件。该配置文件(参看**RFC 2459**)指定”必须/可以/不能”支持的属性，并提供了每个扩展类所用值的取值范围。例如，基本X.509标准没有指定证书暂扣时的指示代码—PKIX定义了相应代码。

(2) 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。 由于每个要求都有不同的服务方式，因此定义了HTTP、LDAP、FTP、X.500等的用法。

PKIX体系结构-续1

(3)**管理协议：这些协议支持不同PKI实体交换信息**(如传递注册请求、撤销状态或交叉证书请求与响应)。管理协议指定实体间浮动的信息结构，还指定处理这些信息所需的细节。管理协议的一个示例是请求证书的证书管理协议(CMP，Certificate Management Protocol)。

(4)**策略大纲：** PKIX在RFC 2527中定义了证书策略(CP，Certificate Policies)和证书实务声明(CPS，Certificate Practice Statements)的大纲，其中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。

(5)**时间标注与数据证书服务：**时间标注服务是由所谓时间标注机构的信任第三方提供的，这个服务的目的是签名消息，保证其在特定日期和时间之间存在，帮助处理不可抵赖争端。数据证书服务(DCS)是信任第三方服务，验证所收到数据的正确性，类似于日常生活中的公证方。

4.4 PKI实例

整个系统由下列子系统构成：

① 签发系统(Authority)；

② 密钥管理中心系统(KMC)；

③ 申请注册系统(RA)；

④ 证书发布系统(DA)；

⑤ 在线证书状态查询系统(OCSP)。

- 由各子系统组成的PKI/CA认证系统的结构如图30所示。

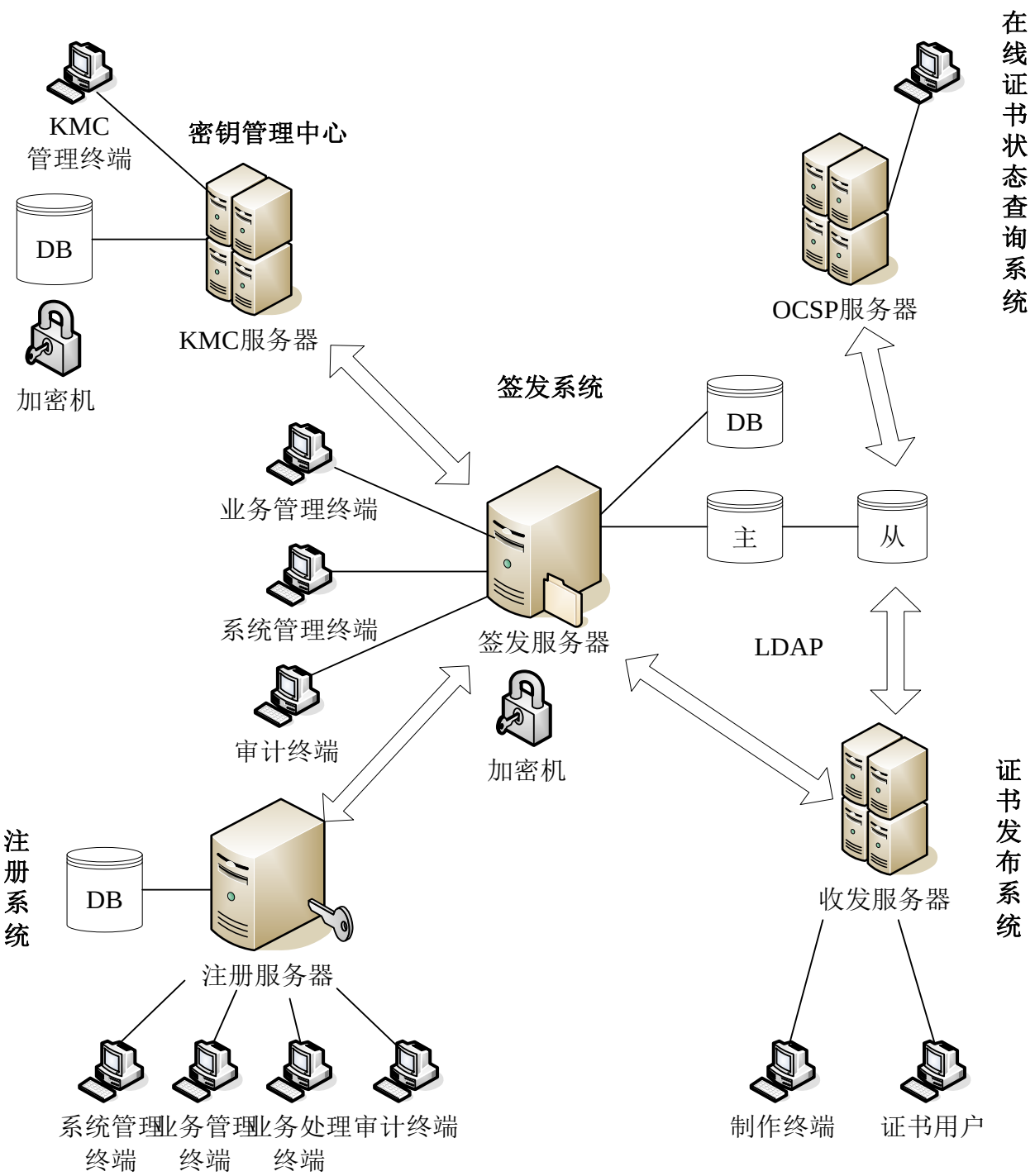


图30 (a)
PKI系统的拓扑结构图

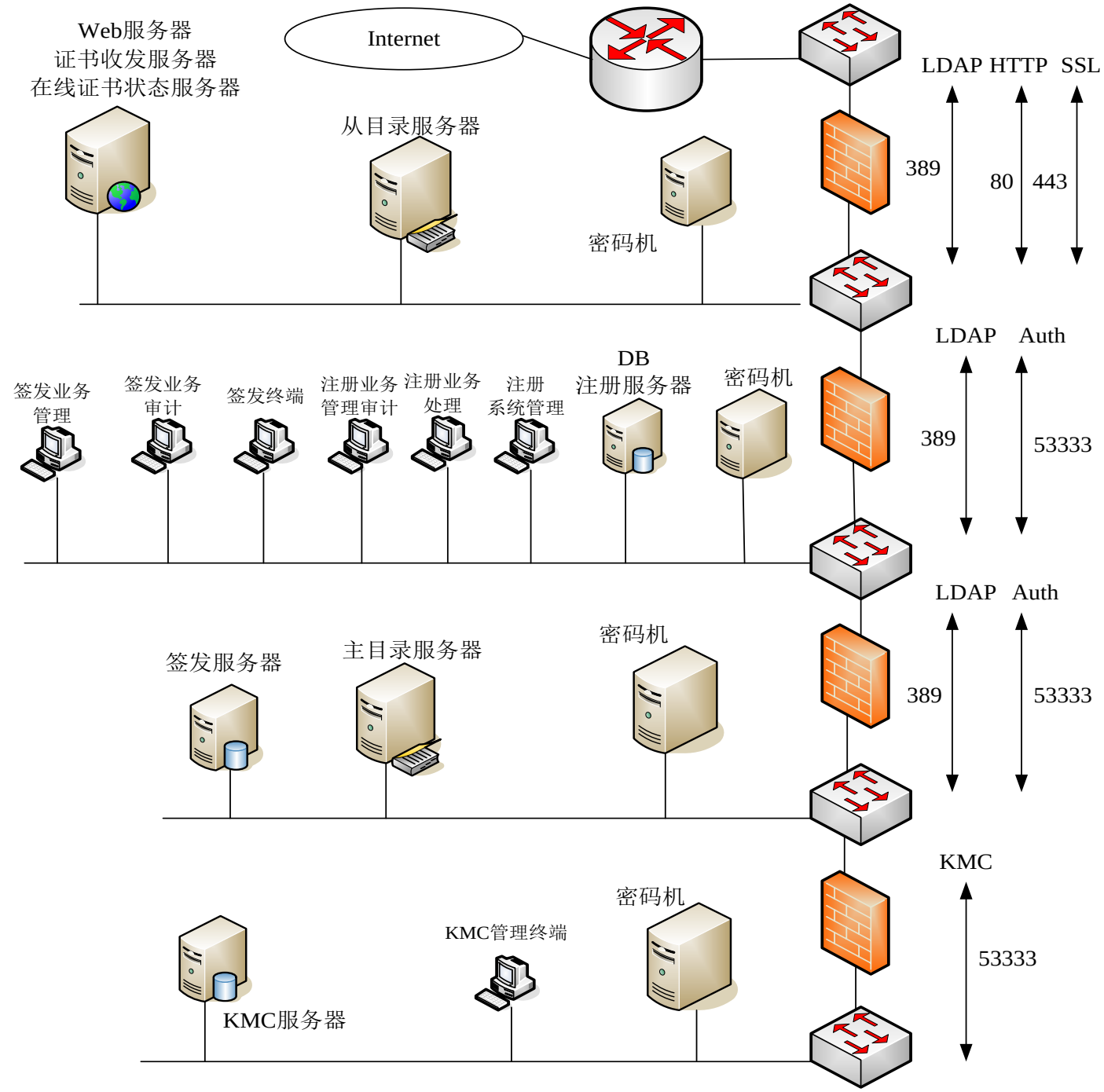


图30 (b)
一个PKI系统实例图