

东南大学网络空间安全学院
密码学与安全协议

第十讲 PKI/CA

黄 杰

信息安全研究中心



知识点:

- 1、公钥基础设施（PKI）的作用
- 2、数字证书及格式
- 3、证书验证方法
- 4、CA中的信任模型



为什么需要公钥基础设施

- 问题1：当你在网上通过交易平台进行交易，或填写真实的信息注册用户时，你首先会想到什么？
 - 1.网站的真实性。
 - 2.信息的机密性。
- 问题2：当你通过**Email**发送报价、标书、财务报告、市场计划等秘密信息时，你有什么样的担心？
 - 1.数据被篡改；
 - 2.信息被窃听；
 - 3.假冒通信方接收了邮件。



为什么需要公钥基础设施

- 问题3：当你在网上下载安装他人发布的软件或插件时，你将有所顾忌吗？
 - 1.代码是否为声称的开发者开发；
 - 2.代码是否被恶意篡改或替换；
 - 3.代码是否注入了病毒程序。



主要内容

- PKI/CA基础
- PKI/CA体系结构
- PKI/CA的技术标准
- 典型的PKI/CA系统
- 典型应用
- 相关资料



- **PKI定义**

- 它是利用公开密钥技术所构建的，解决网络安全问题的，普遍适用的一种基础设施。能够为所有网络应用提供密码服务所需要的证书管理。
- 广义：**PKI** 为全面解决安全问题的基础结构。



- **PKI的发展历程（国际）**
 - **1976年**，提出**RSA**算法
 - **20世纪80年代**，美国学者提出**PKI**的概念
 - **1996年**，美国成立了联邦**PKI**指导委员会
 - **1996年**，**Visa, MasterCard, IBM, Netscape, MS**和数家银行推出**SET**协议，提出证书和**CA**的概念
 - **1999年**，**PKI**论坛成立
 - **2000年4月**，美国国防部宣布采用**PKI**倡议方案
 - **2001年6月13日**，亚洲**PKI**论坛成立



- **PKI的发展历程（国内）**

- **1996-1998**，国内开始电子商务认证方面的研究
- **1997年1月**，科技部下达任务，开始对认证系统
进行研究开发；
- **1998年11月**，湖南**CA**中心开始运作
- **1999年10月**，《商用密码管理条例》颁发
- **2000年**，**CFCA**开始招标并完成
- **2001年**，中国第一家商用**CA**建设完成



PKI/CA 基础



主要内容

- 数字证书
- 目录服务
- 信任模型



数字证书

- 什么是数字证书
- X.509数字证书
- 证书验证
- 数字证书生命周期
 - 数字证书的使用
 - 数字证书的存储
 - 数字证书的撤销



什么是数字证书

- 数字证书（**Digital ID**），又叫“数字身份证”、“网络身份证”，是由认证中心发放并经认证中心数字签名的，包含公开密钥拥有者以及公开密钥相关信息的一种电子文件，可以用来证明数字证书持有者的真实身份。
- 数字证书采用公钥体制。
- 数字证书的格式一般采用**X.509**国际标准。

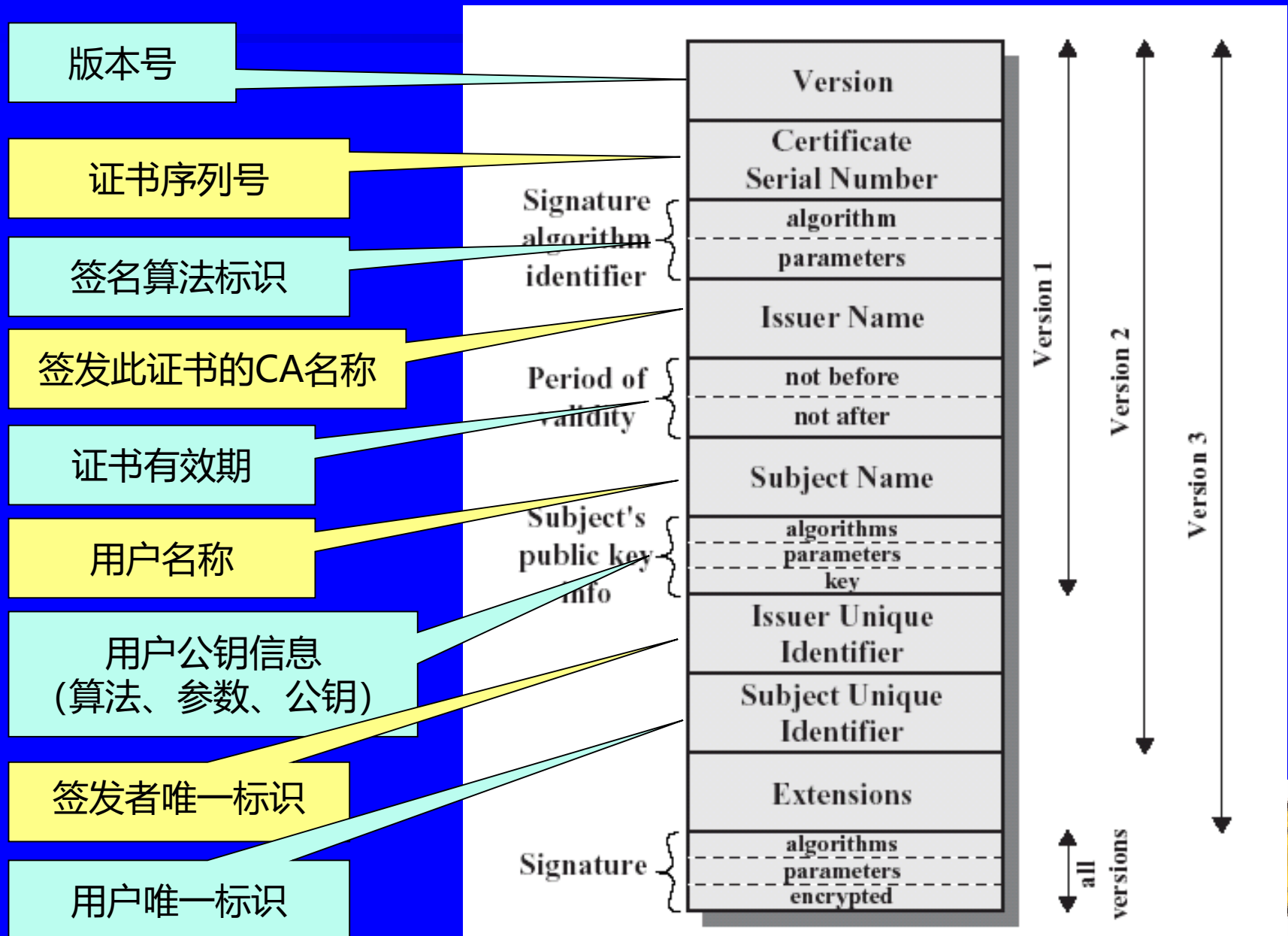


X.509数字证书

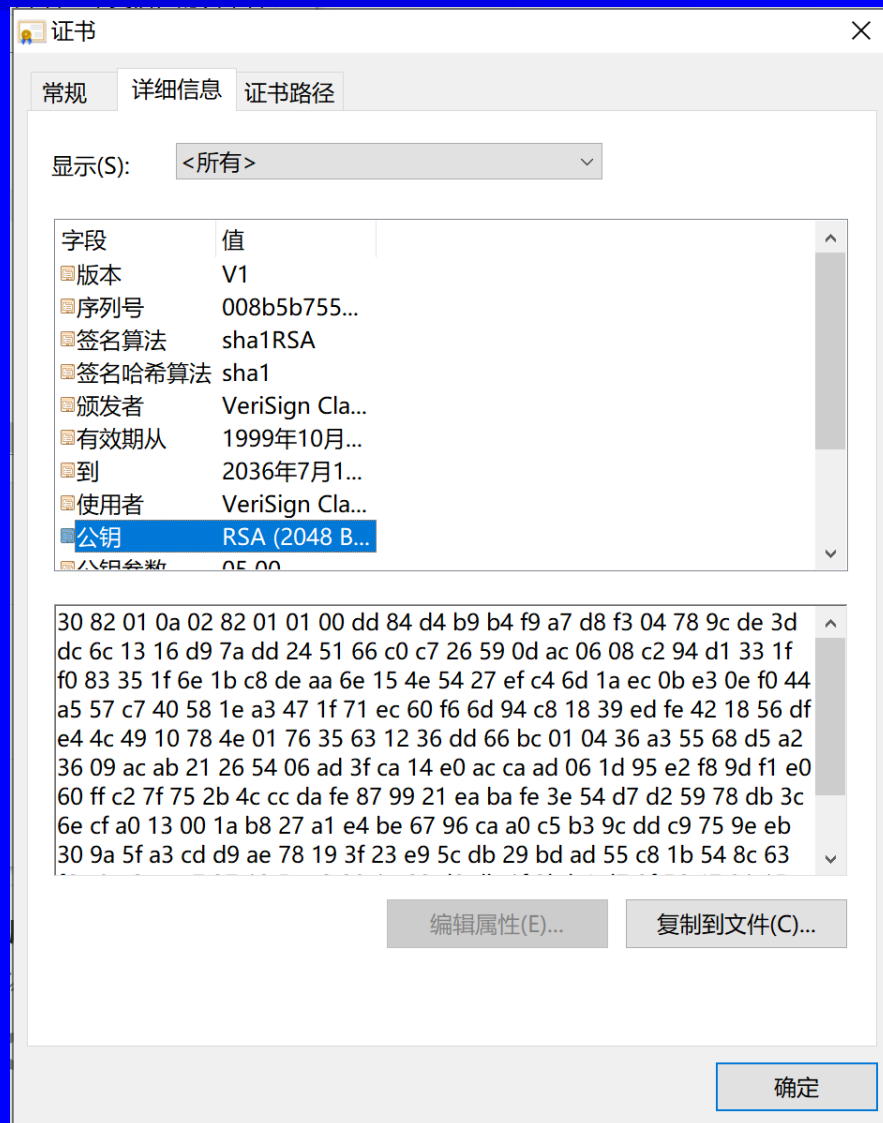
- **X.509, ITU-T Recommendation: Information Technology – Open System Interconnection – The Directory: Authentication Framework**
- **X.509是X.500标准系列的一部分，在PKI的发展中，X.509起到了无可比拟的作用.**
- **X.509定义并标准化了一个通用的、灵活的证书格式.**
- **X.509的实用性来源于它为X.509 v3和X.509 v2 CRL定义的强有力的扩展机制.**



X.509数字证书



X.509数字证书

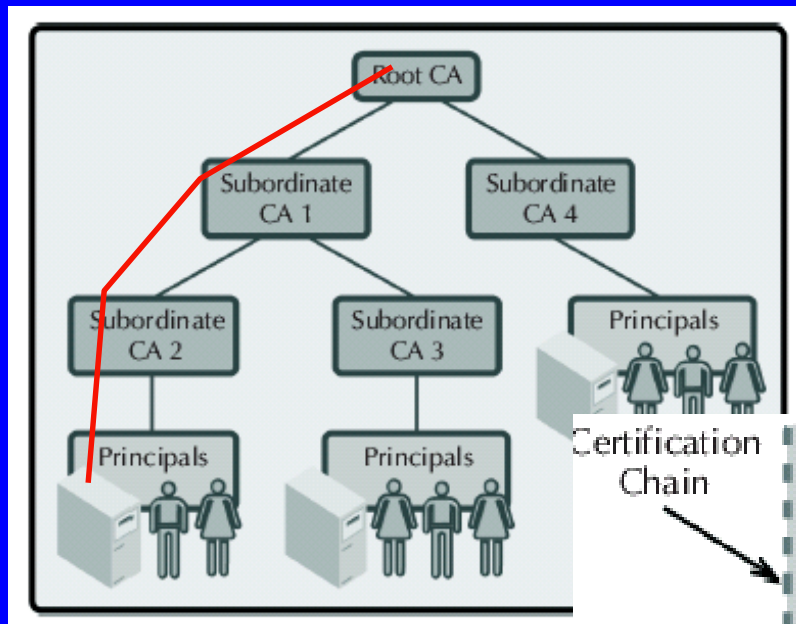


证书验证

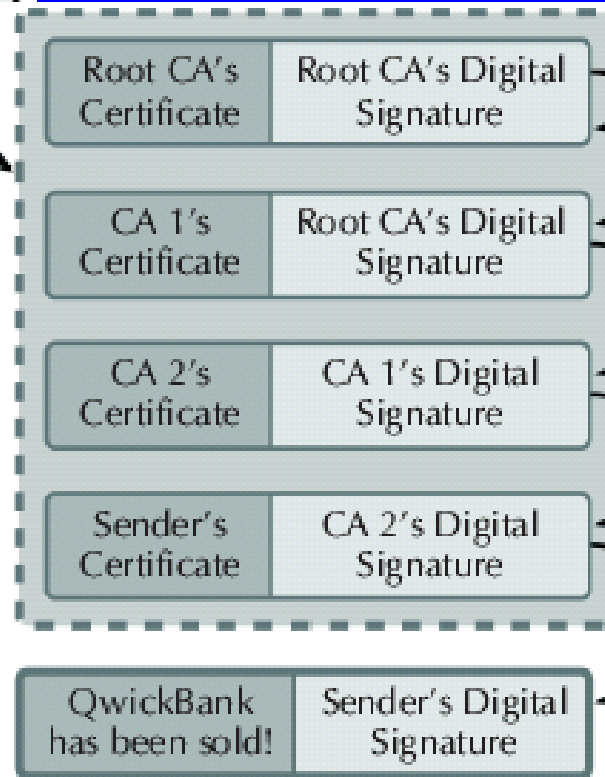
- 当证书持有者A想与证书持有者B通信时，他首先查找数据库并得到一个从证书持有者A到证书持有者B的证书路径和证书持有者B的公钥。这时证书持有者A可使用单向或双向验证证书。
- 单向验证是从证书持有者A到证书持有者B的单向通信。
- 双向验证与单向验证类似，但它增加了来自证书持有者B的应答。



证书链的验证示例



Certification Chain



- 1) Extract root CA's public key and verify both root CA signatures
- 2) Extract CA 1's public key and verify CA 1's signature
- 3) Extract CA 2's public key and verify CA 2's signature
- 4) Extract sender's public key and verify sender's signature

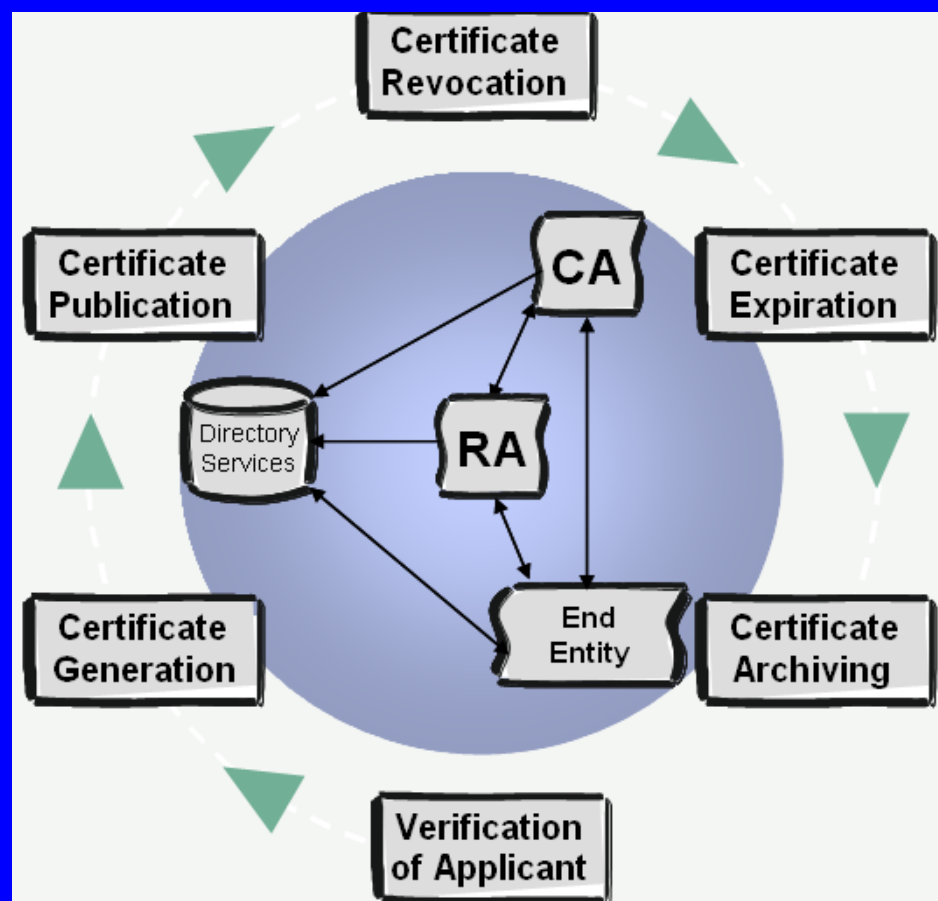
证书验证与证书生命周期

- 证书有效性或可用性验证
- 证书生命周期
- **初始化阶段**: 终端实体注册->密钥对产生->证书创建和证书分发, 证书分发, 证书备份
- **颁发阶段**: 证书检索, 证书验证, 证书恢复, 证书更新
- **撤销阶段**: 证书过期, 证书恢复, 证书撤销, 证书档案



数字证书生命周期

- 证书申请
- 证书生成
- 证书存储
- 证书发布
- 证书使用
- 证书撤销
- 证书更新
- 证书备份
- 证书检索
- 证书恢复
- 证书归档



数字证书的使用

- 每一个用户有一个各不相同的名称，一个可信的认证中心CA给每个用户分配一个唯一的名称并签发一个包含用户名称和公钥的证书。
- 证书可以存储在数据库中。用户可以利用网络彼此交换证书。当证书撤销后，它将从证书目录中删除，然而签发此证书的CA仍保留此证书的副本，以备日后解决可能引起的纠纷。



数字证书的存储

- 数字证书可以存放在计算机硬盘、软盘、IC卡或CPU卡中。
- 数字证书在计算机硬盘中存放时，使用方便，但存放证书的计算机必须受到安全保护。
- 软盘保存证书，被窃取的可能性有所降低，但软盘容易损坏，易于导致用户数字证书的不可用。
- 使用IC卡存放证书成本较低，且本身不易被损坏，安全强度较高，成为目前较为广泛的一种数字证书存储方式。
- 使用CPU卡存放证书时，安全级别最高，但相对来说，成本较高。



数字证书的撤销

- **证书撤销原因**：当证书还没过期时无效的时候，需要撤销证书。
- **证书撤销列表（CRL）**：所有被撤销的但还没过期的证书序列号列表。
- **CRL由CA整理并签发**。
- **CRL需周期性更新**。必须在公布的目录中是可用的，以备用户使用。
- **增量CRL**：为了防止频繁地更新CRL的一种机制。增量CRL包含了CRL的更新部分，从最近的前一版本CRL或者增量CRL算起撤销的那部分。例如，CRL可能一个月颁发一次，而增量CRL是24小时颁布一次。



目录服务

- 目录是网络系统中各种资源的清单，保存了网络中用户、服务器、客户机、交换机、打印机等资源的详细信息，同时还收集了这些资源之间各种复杂的相互关联关系。
- 证书和证书吊销列表(CRL)的存储(主要针对X.509格式来说)是X.500和目录服务标准的主题。



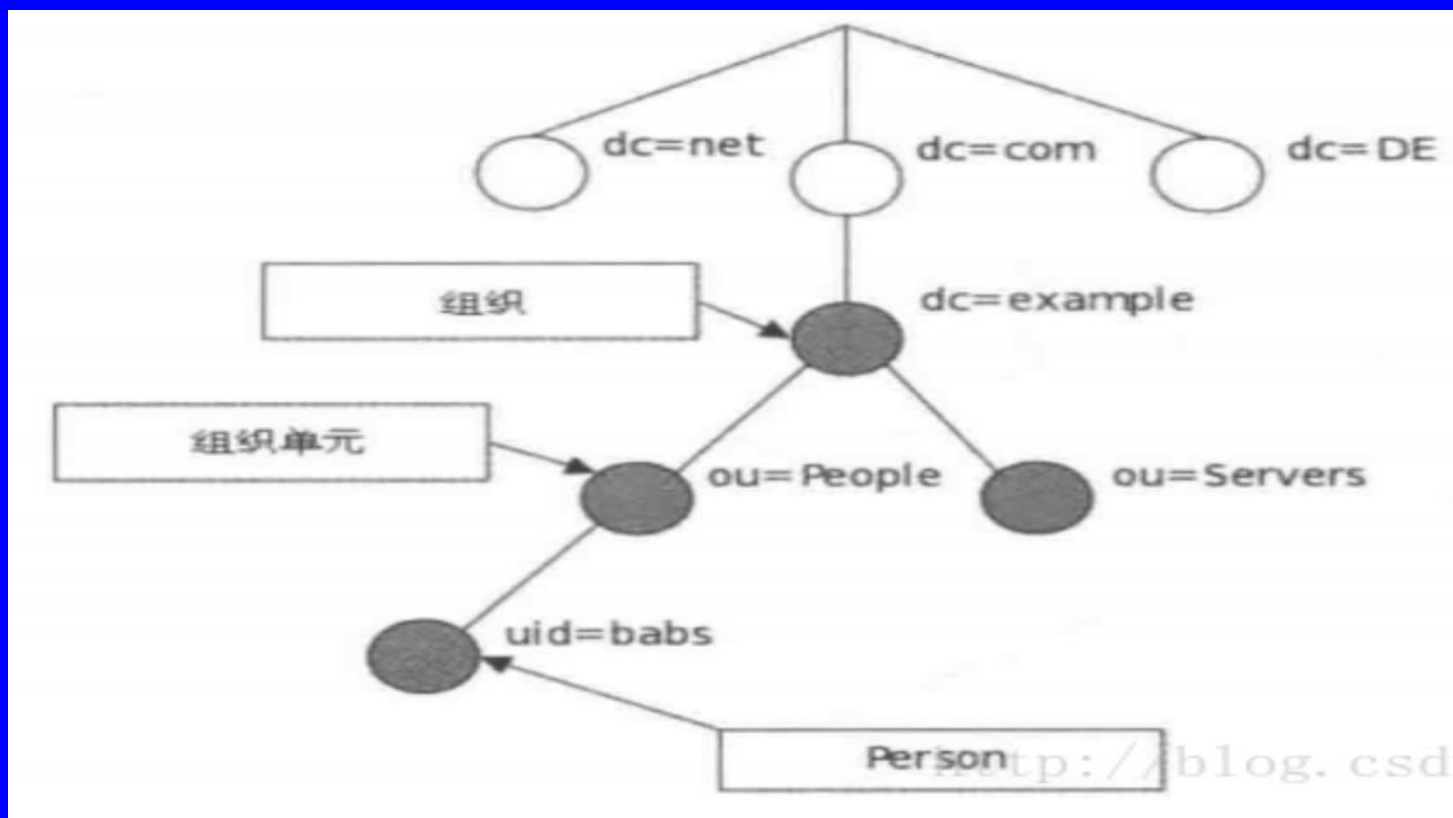
X.500目录服务

- **X.500, ITU-T Recommendation: The Directory – Overview of Concepts and Models.**
- **X.500目录服务是一个高度复杂的信息存储机制，包括客户机-目录服务器访问协议、服务器-服务器通信协议、完全或部分的目录数据复制、服务器链对查询的响应、复杂搜寻的过滤功能等。**



LDAP目录服务

- LDAP是X.500的简化实现
- LDAP目录的条目（**entry**）由属性（**attribute**）的一个集合组成，并由一个唯一性的名字引用，即专有名称（**distinguished name, DN**）。



信任模型

- 通常证书并不由一个CA直接签发，而是从被信任的CA到一个给定的证书有一个证书路径。例如：
 - 根CA的证书C0(由根CA签发)：根CA是被信任的
 - A1的证书C1(由根CA签发)
 - A2的证书C2(A1签发)
 - ...
 - An-1的证书Cn-1(由An-3签发)
 - An的证书Cn(由An-1签发)
- 通过依次验证证书C1, C2, ..., Cn来验证Cn是可信的，即证书链。



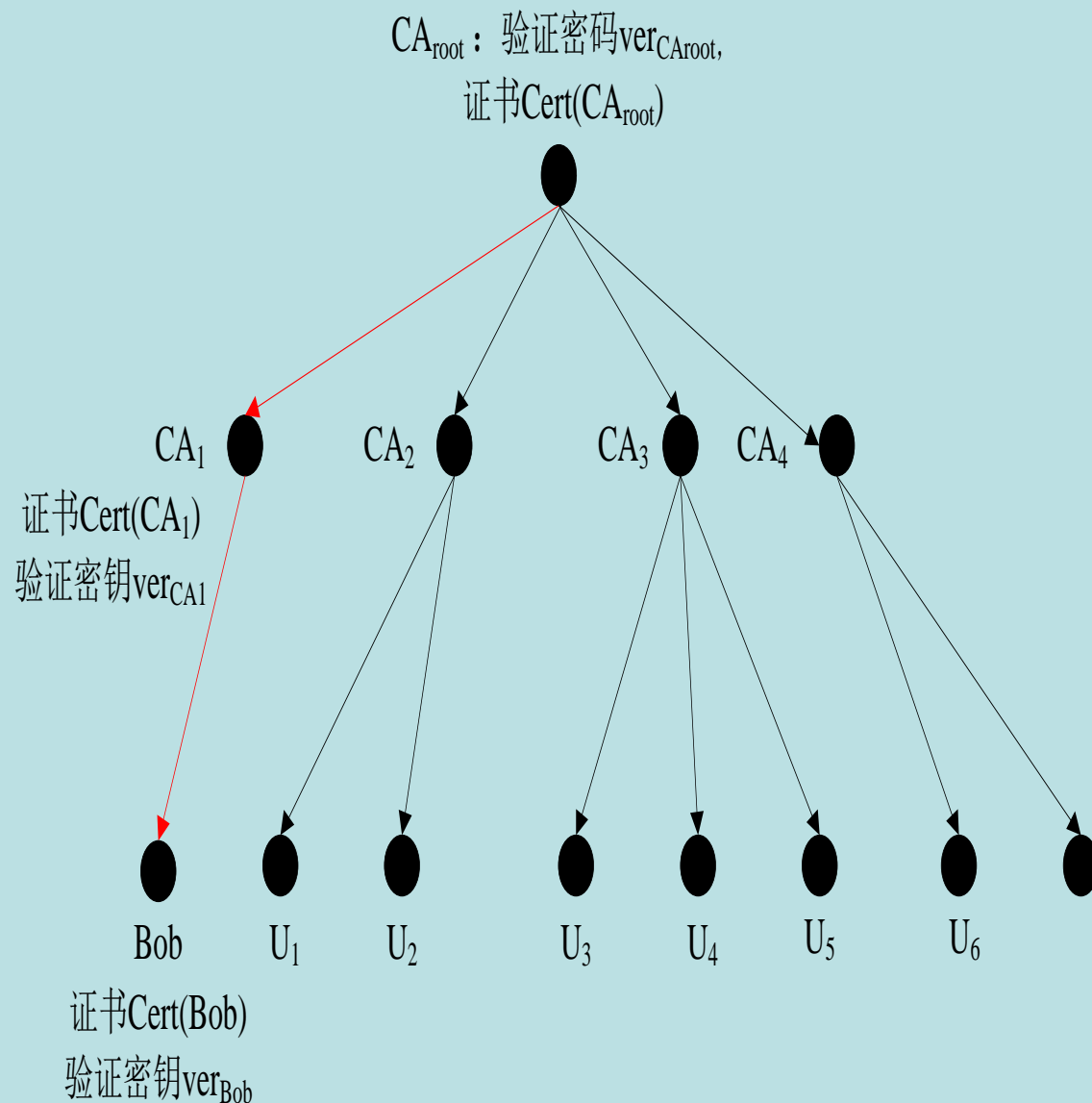
信任模型

- 信任模型规定了证书链应该如何构造的规则。
- 信任模型类型
 - 严格层次模型
 - 网络化模型
 - 用户为中心的模型（即**PGP**信任模型）



信任模型1——严格层次模型

- 在严格层次模型中，根CA有个自签名的，自颁发的证书。根CA被称为信任锚。
- 根CA可以给下级CA颁发证书，而任何CA可以给终端用户颁发证书。
- 证书链：从根CA开始，到需验证的用户证书，这条路径上的所有证书依次构成证书链。



根CA和下层CA的作用

- 根CA

- 发布本**PKI**信任域的认证策略;
- 发布自身证书;
- 签发和管理下层**CA**证书;
- 对下层**CA**进行身份认证和鉴别;
- 废除所签发的证书;
- 为所签发的证书产生**CRL**;
- 发布所签发的证书和**CRL**;
- 保存证书、**CRL**以及审计信息;
- 密钥安全生成及管理;
- 实现交叉认证。



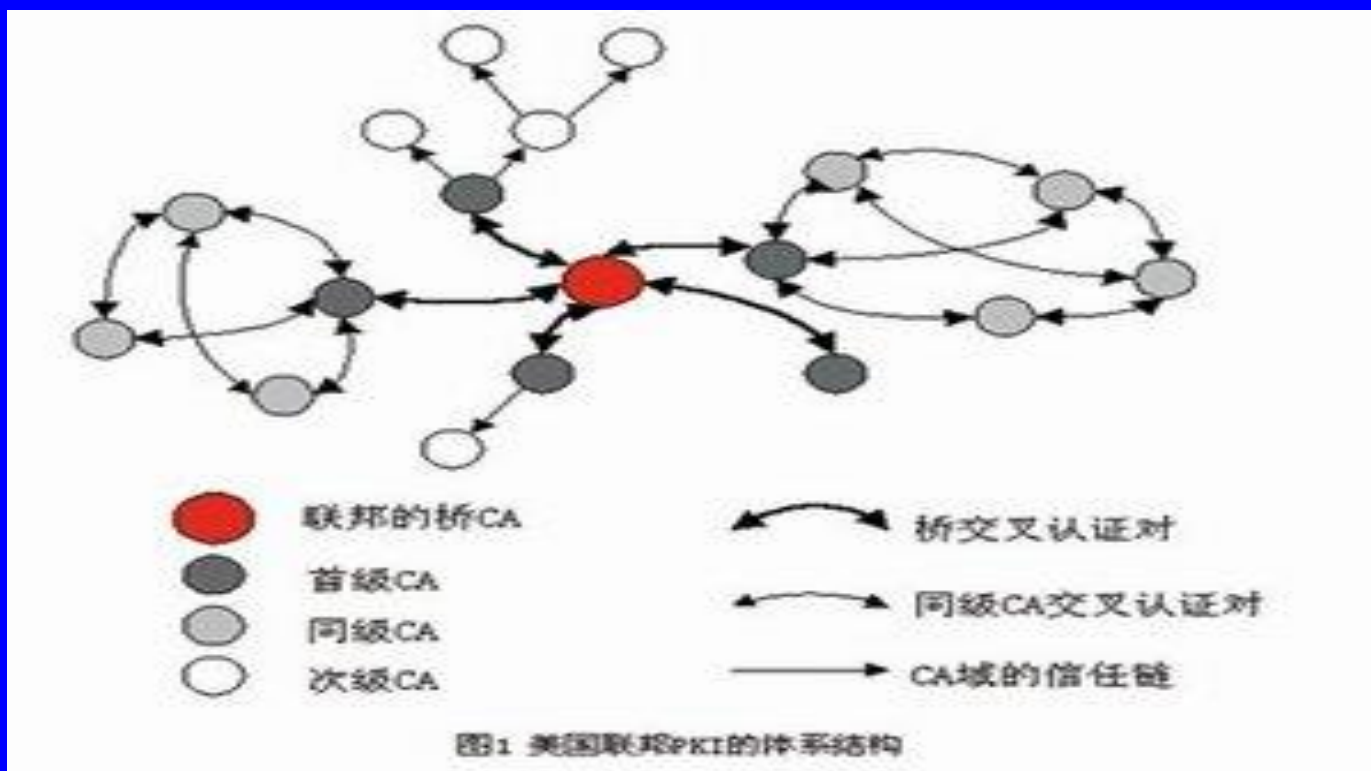
• 下层CA

- 发布本地CA对根CA政策的增补部分；
- 对下属机构进行认证和鉴别；
- 产生和管理下属机构的证书；
- 发布自身证书；
- 证实RA的证书申请请求；
- 向RA返回证书制作的确认信息或已制定好的证书；
- 接收和认证对它所签发的证书的作废申请请求；
- 为它所签发的证书产生CRL；
- 保存证书、CRL、审计信息和它所签发的政策；
- 发布它所签发的证书和CRL；
- 密钥安全生成及管理；
- 实现交叉认证。



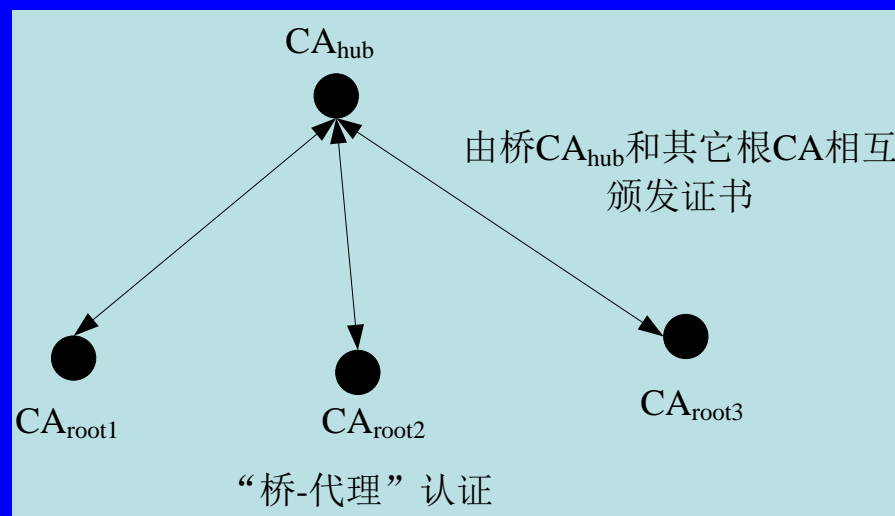
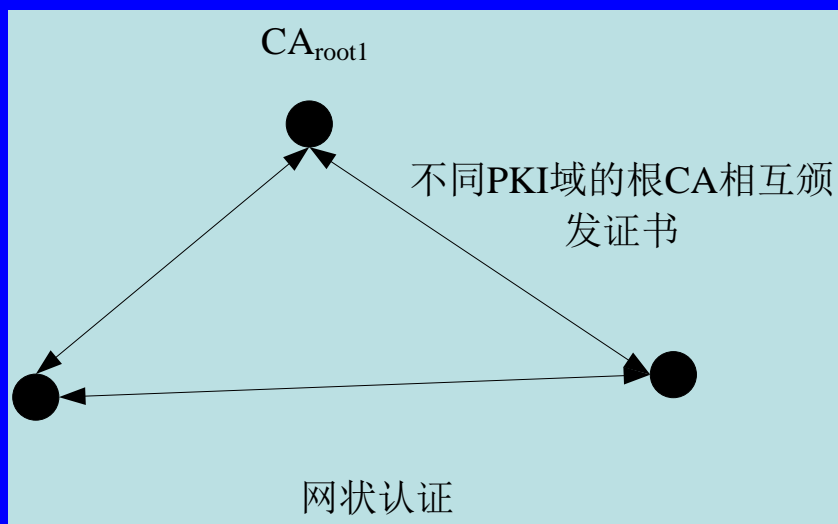
信任模型2——网络化模型

- 网络化模型用来连接两个不同的**PKI**域的根**CA**，这样属于不同**PKI**域的用户证书可以相互认证。
- 网络化模型中不同**PKI**域的信任模型不一定相同。
- 交叉认证：不同域的**CA**相互颁发证书



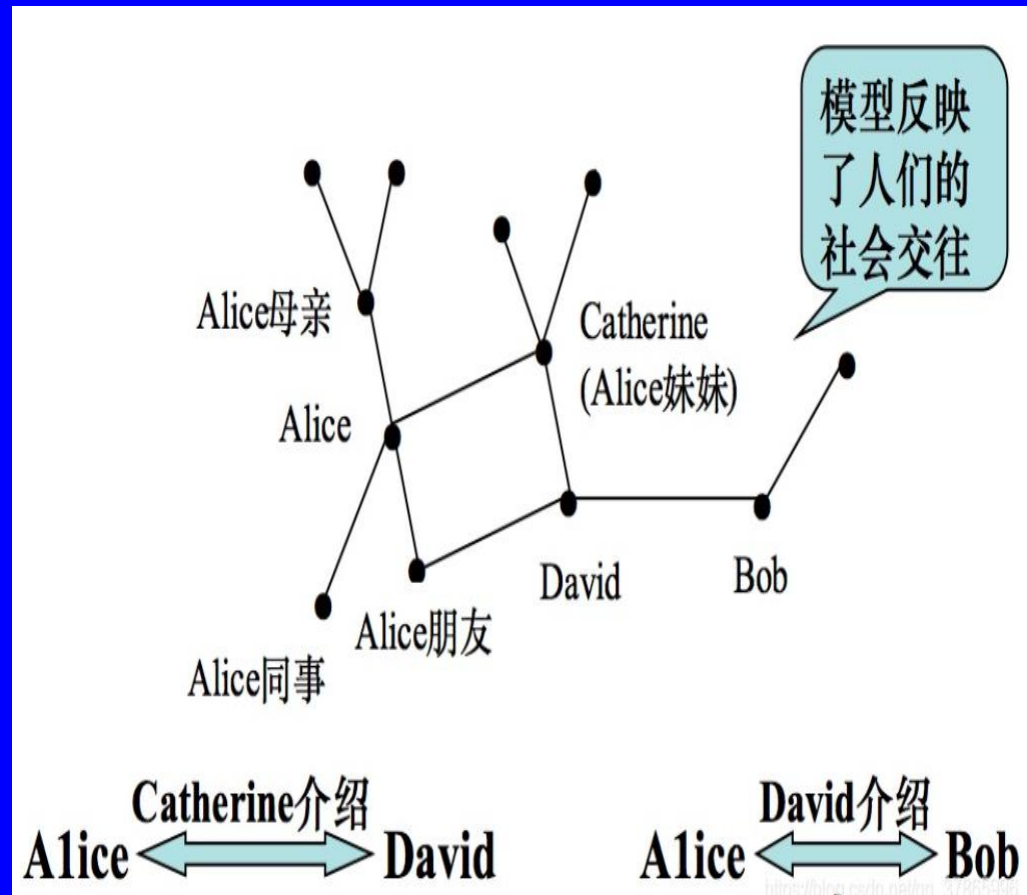
信任模型2——网络化PKI模型

- 不同PKI域的CA交叉认证方法：
 - 网状认证
 - “桥-代理”认证
- 如何构造证书路径：**Alice**为了验证**Bob**的证书，那么**Alice**需要找到从**Alice**的信任锚到**Bob**的信任路径。



信任模型3——用户为中心的模型

- 每个用户自己决定信任其他哪些用户。
- 用户的最初信任对象包括用户的朋友/家人/同事，但是否真正信任某证书则被许多因素所左右。
- PGP的一个用户通过担当CA（签发其他实体的公钥）来发布其他实体的公钥来建立信任网（Web of Trust）。

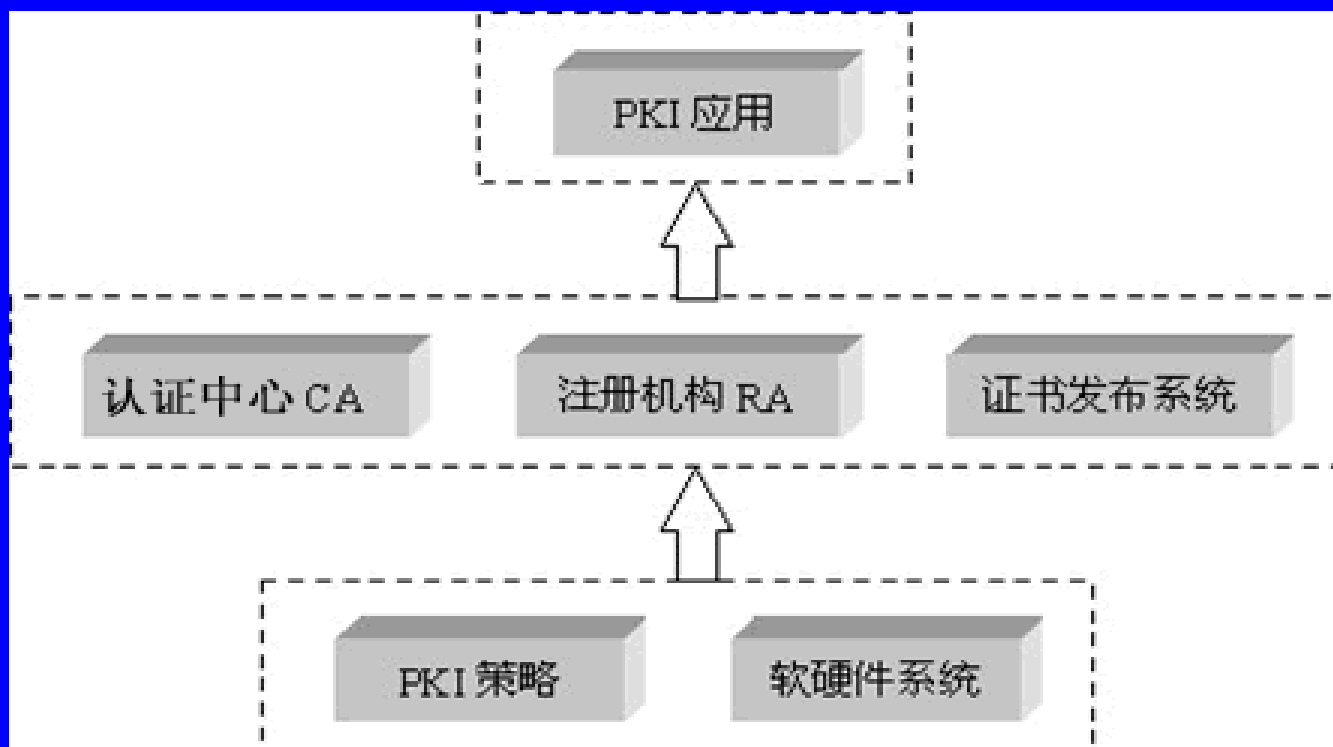


PKI/CA 体系结构

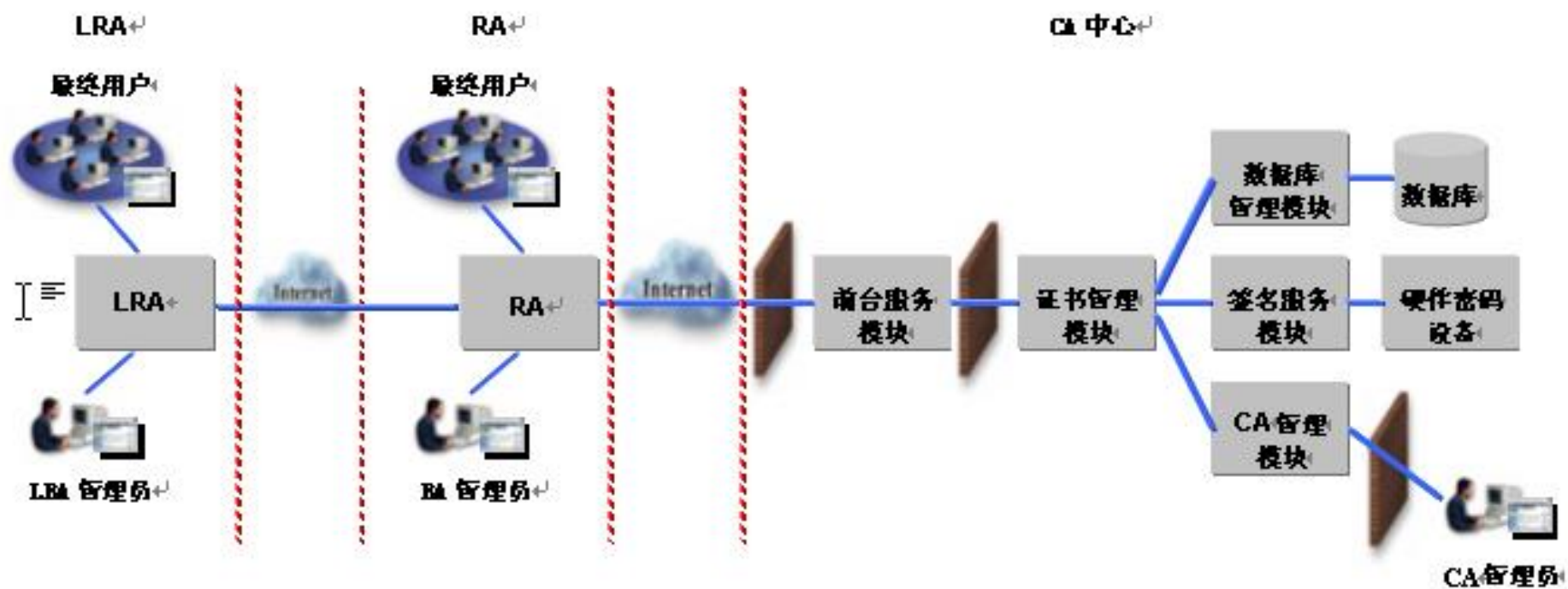


PKI及其组成

- **PKI**是生成、管理、存储、分发和撤销基于公钥密码学的公钥证书所需要的硬件、软件、人员、策略和规程的总和。
- **PKI**的构件，**PKI**的安全策略



CA的网络结构



认证中心CA

- 可信的第三方
- 主要功能
 - 证书申请，接收并验证最终用户数字证书的申请；
 - 证书审批，确定是否接受最终用户数字证书的申请；
 - 证书签发，向申请者颁发、拒绝颁发数字证书；
 - 证书更新，接收、处理最终用户的数字证书更新请求
 - 接收最终用户数字证书的查询、撤销；
 - 产生和发布证书废止列表（**CRL**），验证证书状态；
 - 提供**OCSP**在线证书查询服务，验证证书状态；
 - 提供目录服务，可以查询用户证书的相关信息；
 - 下级认证机构证书及帐户管理；
 - ...



- 注册机构**RA**

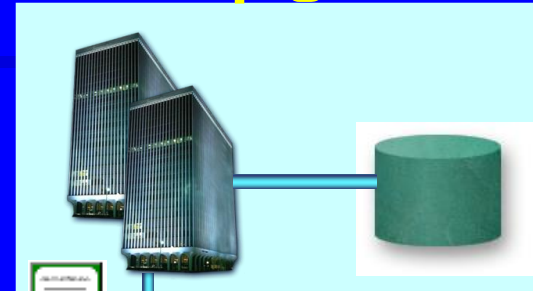
- 自身密钥的管理，包括密钥的更新、保存、使用、销毁等；
- 审核用户信息；
- 登记黑名单；
- 业务受理点**LRA**的全面管理；
- 接收并处理来自受理点的各种请求。

- 业务受理点**LRA**

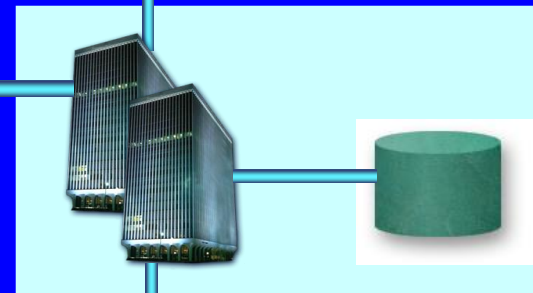
- 受理用户的证书申请及废除请求；
- 录入用户的证书申请及废除请求；
- 审核用户的证书申请及废除请求资料；
- 对用户的证书申请及废除请求进行批准或否决；
- 提供证书制作。



CA中心



Cert ↓ ↑ CSR



RA



证书最终用户



证书最终用户



RA管理员



CP与CPS

- **CP, Certificate Policy**
 - 定义了一个用户对其它用户数字证书信任的程度
- **CPS, Certification Practice Statement**
 - 人们与组织根据CA的CPS来确定他们对该CA的信任程度
- **RFC 3647**
 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

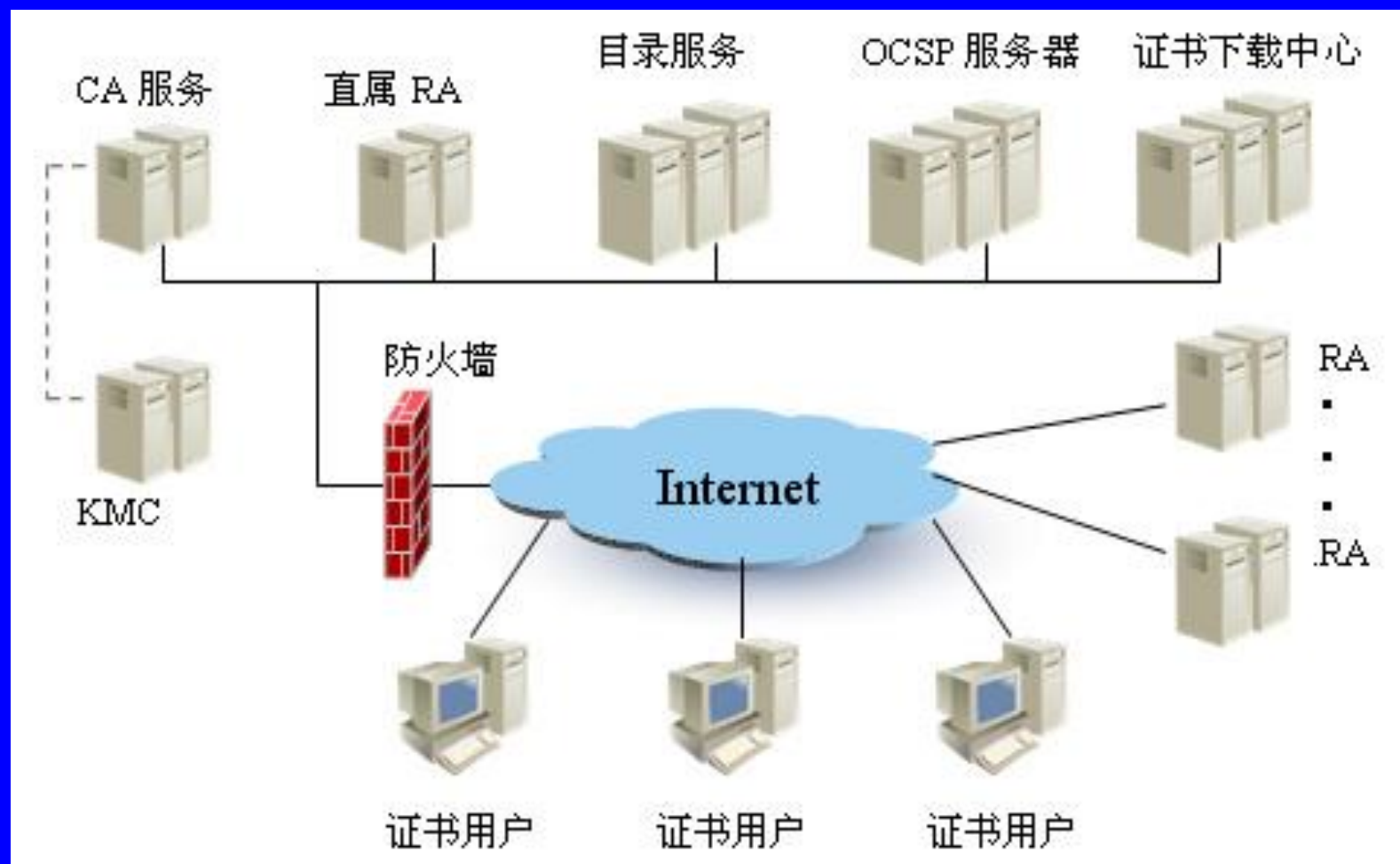


构建PKI的两种模式

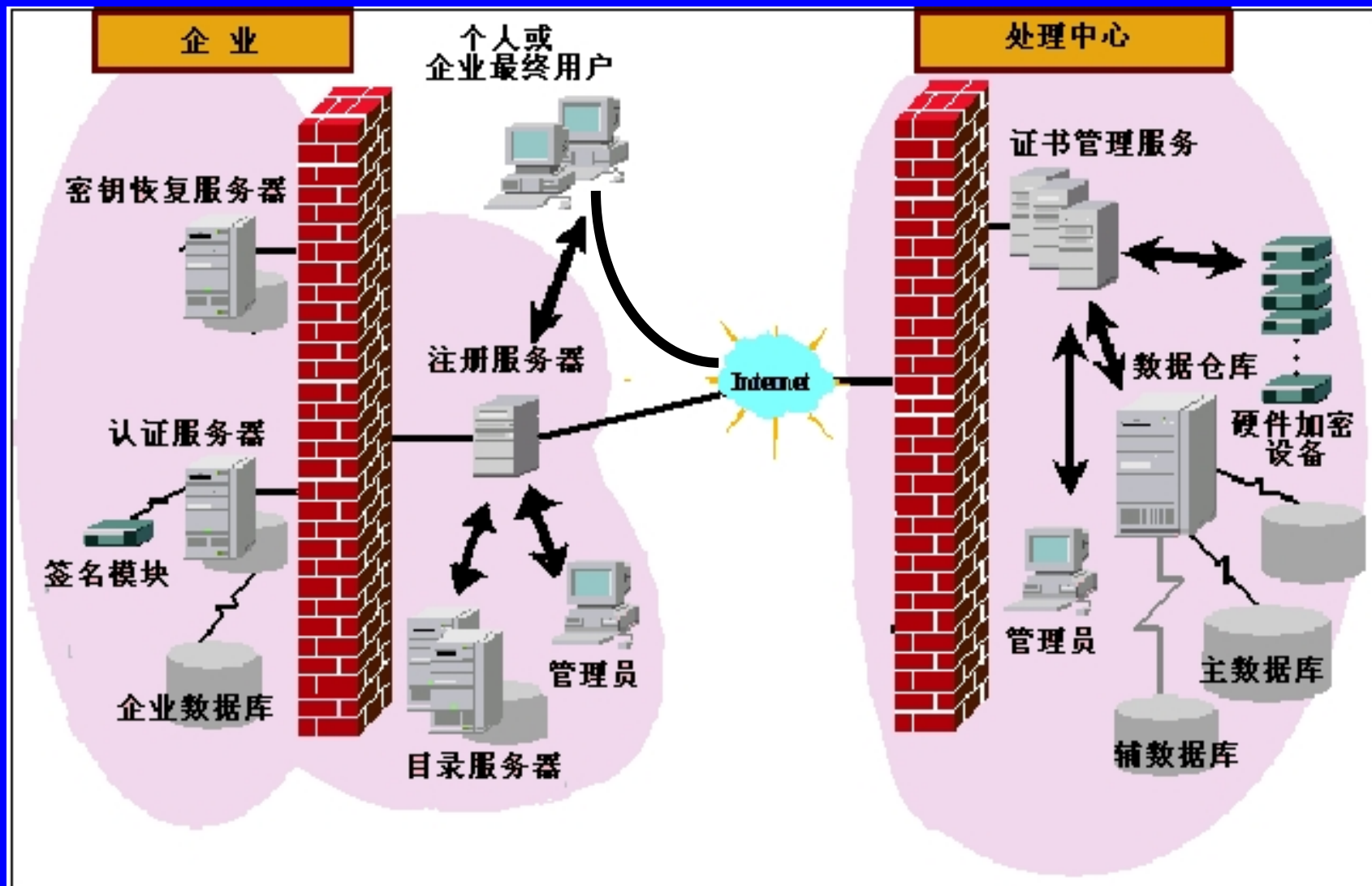
- 自建模式
- 托管模式



典型的自建系统



典型的托管系统



PKI涉及到的法律问题

- 数字签名的法律状况
- **PKI**的法律框架
- 许可权，角色与责任，私有**PKI**(企业**PKI**)
- 密码管理政策与法规(不同的密码管理政策)



国外PKI相关法律建设状况

- 联合国
 - 《电子商务示范法》
 - 《电子签章统一规则草案》
- 美国
 - 《全球及全国电子商务电子签章法案》
- 欧盟
 - “欧洲电子商务倡议书”
- 亚州
 - 新加坡、韩国、日本、香港、台湾



PKI/CA 技术标准



ITU-T X.509及相关标准

- ITU-T X.509 Edition 1
- ITU-T X.509 Edition 2
- ITU-T X.509 Edition 3
- ITU-T X.509 Edition 4
- ITU-T的其他标准



PKIX系列标准

- 证书和CRL标准: RFC2459
- PKI体系中的操作协议: RFC2559, RFC2560, RFC2585
- PKI管理协议: RFC2510, RFC2511, RFC2797
- 证书管理的政策和证书操作规范: RFC2527
- 提供防抵赖的时戳和数据认证服务: RFC3029, RFC3161



典型的PKI/CA 系统



- 商业应用
- 政府应用

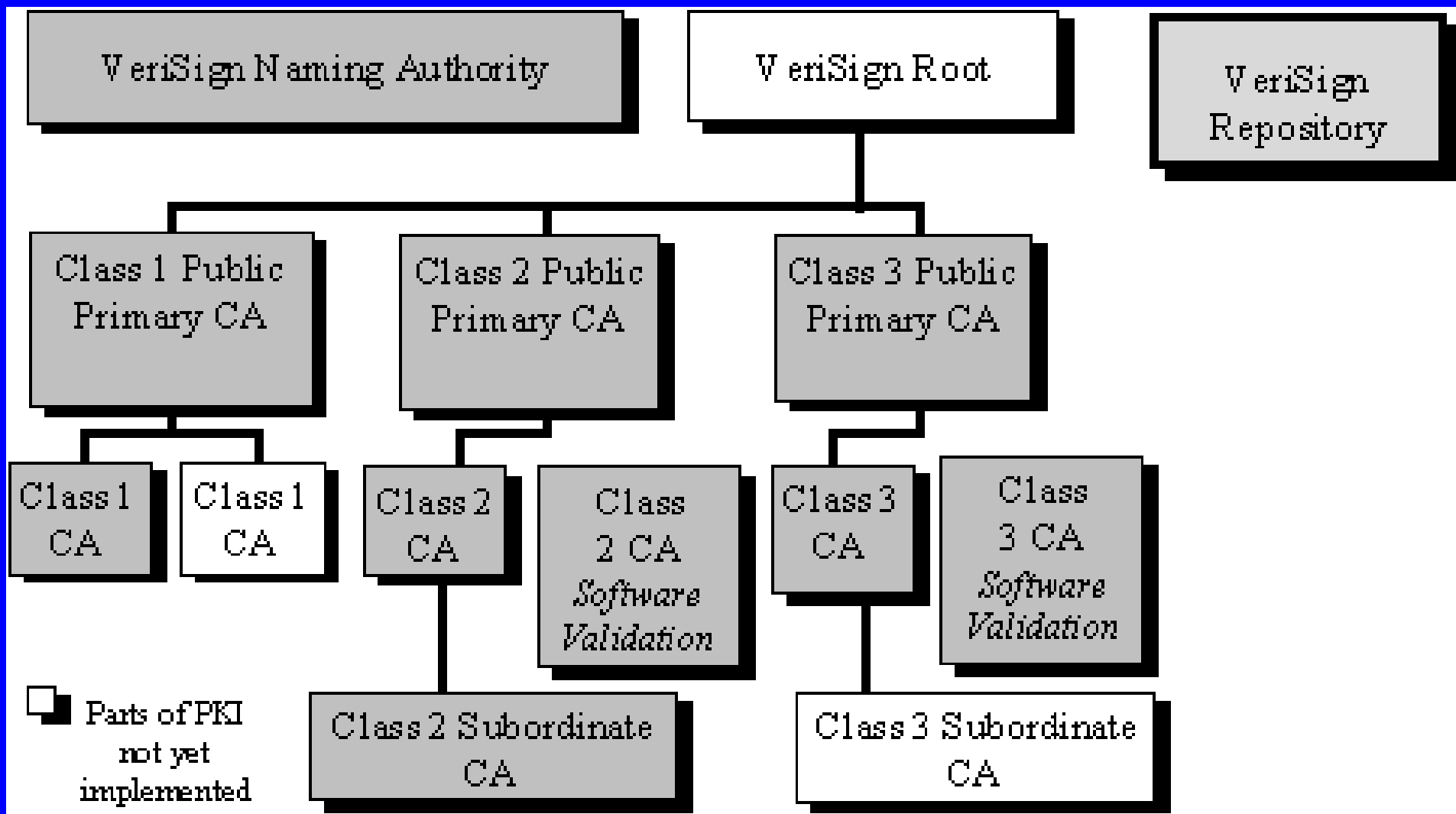


商业应用

- VeriSign (<http://www.verisign.com/>)
- Entrust (<http://www.entrust.com/>)
- Baltimore (<http://www.baltimore.com/>)
- RSA Security
(<http://www.rsasecurity.com/>)



VeriSign PKI层次图



VeriSign Key Hierarchy

1. Root Level

2. PCA Level

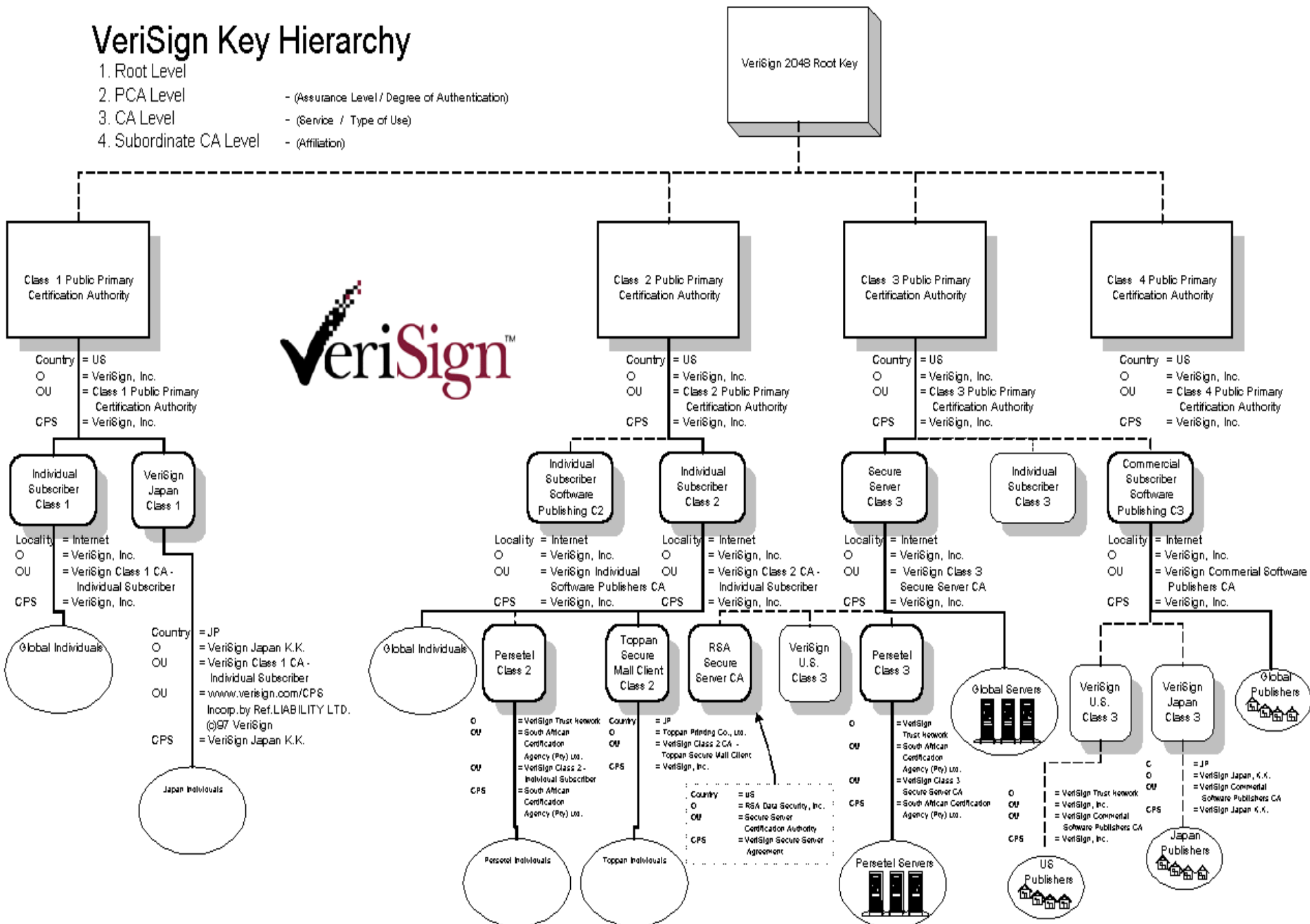
3. CA Level

4. Subordinate CA Level

- (Assurance Level / Degree of Authentication)

- (Service / Type of Use)

- (Affiliation)



Note: This VeriSign Key Hierarchy does not necessarily include all issuing authorities and other entities within the hierarchy. VeriSign makes no warranties with respect to its accuracy or otherwise. No part of this document may be reproduced in part or in full without the prior written permission of VeriSign.

典型应用



- **Web的安全服务**
- **安全电子邮件（ S/MIME ）**
- **安全电子交易（SET）**



Web安全服务

- 安全问题：
欺诈、泄露、篡改、攻击



使用PKI系统的对策

- SSL: 由Netscape公司研究制定, 该协议向基于TCP / IP的客户及服务器应用程序提供了客户端和服务器的鉴别、信息机密性及完整性等安全措施。
- SSL主要提供三方面的服务
 - 认证用户和服务器
 - 加密数据以隐藏被传送的数据
 - 维护数据的完整性

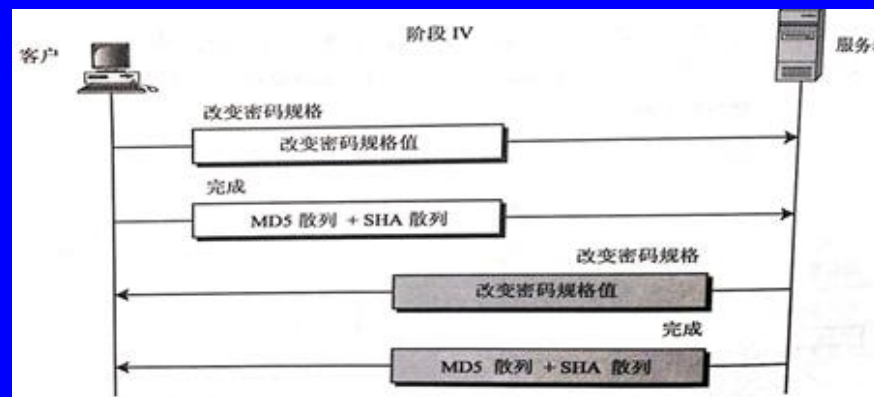
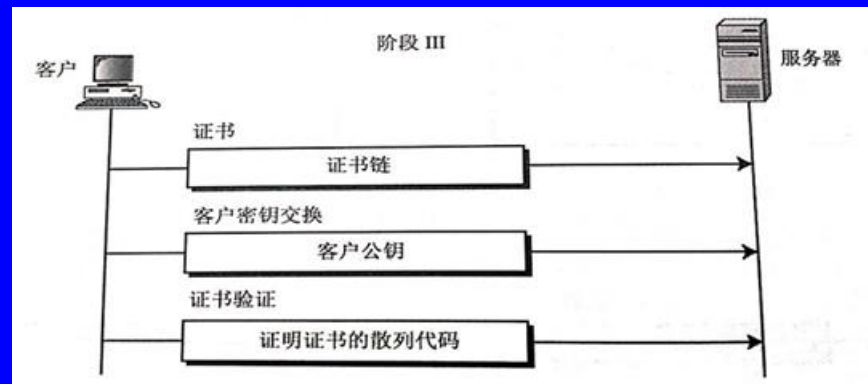
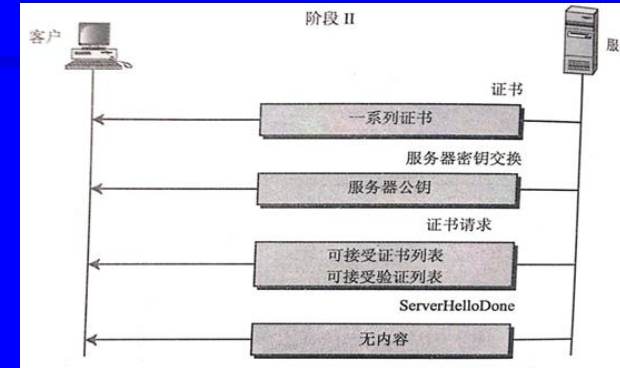
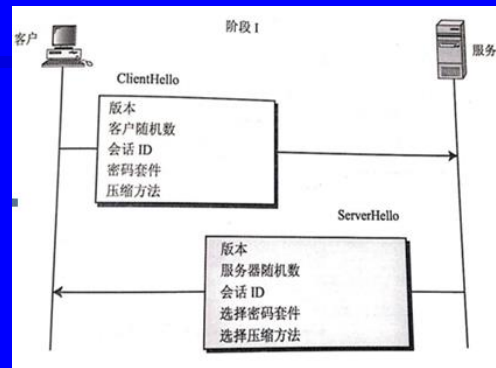
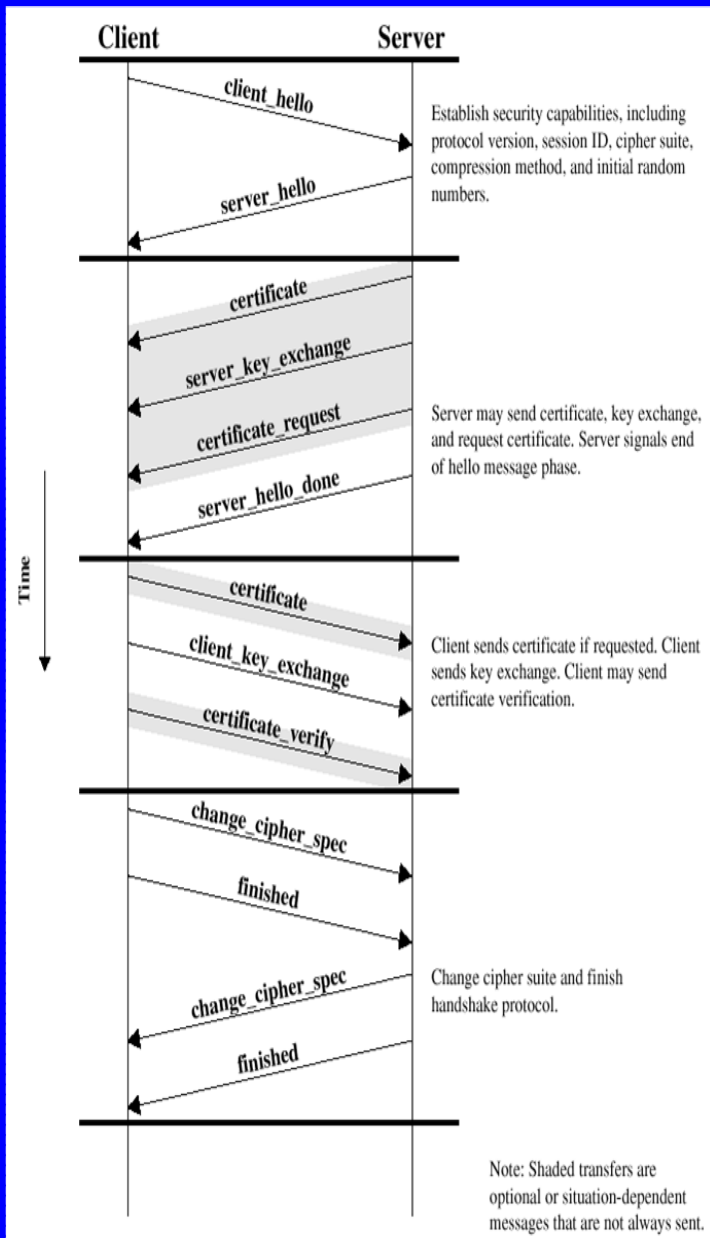


SSL/TLS

- 由Netscape, IETF TLS工作组开发
- **SSL/TLS**在源和目的实体间建立了一条安全通道(在传输层之上), 提供基于证书的认证、信息完整性和数据保密性
- **SSL体系结构: SSL协议栈**



SSL/TLS



安全电子邮件

- 安全电子邮件实现原理
 - 安全电子邮件实现方案
- S/MIME**



安全电子邮件实现原理


在安全的电子邮件系统中，收发双方都有双方的数字证书。发送方是在电子邮件的附件中增加发信者的数字签字，同时也可将邮件内容用对方的公钥加密。用户在收到电子邮件后，电子邮件系统对加密的邮件会自动解密，同时自动验证该邮件的数字签字并将结果通知用户，从而大大地提高了电子邮件的保密性和可信性。



选项

首选参数 | 邮件服务 | 邮件格式 | 拼写检查 | 安全 | 其他 | Internet 电子


安全电子邮件


 ☒ 将待发邮件的内容和附件加密 (E)
☒ 给待发邮件添加数字签名 (Q)
☒ 发送文字签名邮件 (T)

默认安全设置 (E): 我的 S/MIME 设置


更改设置 (S)...

安全内容

 安全区域用于自定义是否可在 HTML 邮件中运行脚本和活动内容。请选用 Internet Explorer 安全区域。

区域 (Z):  Internet 区域设置 (N)...
附件的安全性 (C)...

数字标识 (证书)

 数字标识或证书是一种可让您在电子商务中证实身份的文档。

导入/导出数字标识 (I)... 获取数字标识 (G)...

确定 取消 应用 (A)

更改安全性设置

安全性设置优先级

安全设置名称 (S): 我的 S/MIME 设置

安全邮件格式 (E): S/MIME

☒ 该安全邮件格式的默认安全性设置 (T)
☒ 所有安全邮件的默认安全性设置 (M)

新建 (N) 删除 (D) 密码 (P)...

证书和算法

签名证书: Dong You 选择 (C)...

签名算法 (A): SHA1

加密证书: Dong You 选择 (H)...

加密算法 (L): 3DES

☒ 将证书与签名的邮件一同发送 (E)

确定 取消



安全电子交易SET

- 1996年2月，IBM, Microsoft, Netscape, RSA, Terisa和VeriSign开发了SET v1(针对MasterCard和Visa安全标准的需要而出现的)
- SET是开放的、设计用来保护Internet上信用卡交易的加密和安全规范
- 从本质上，SET提供了三种服务：
 - 在交易涉及的各方之间提供安全的通信信道
 - 通过使用X.509 v3数字证书来提供信任。
 - 保证机密性，因为信息只是在必要的时候、必要的地方才对交易各方可用
- 交易过程：购买请求、支付认可和支付获取



SET的主要特征

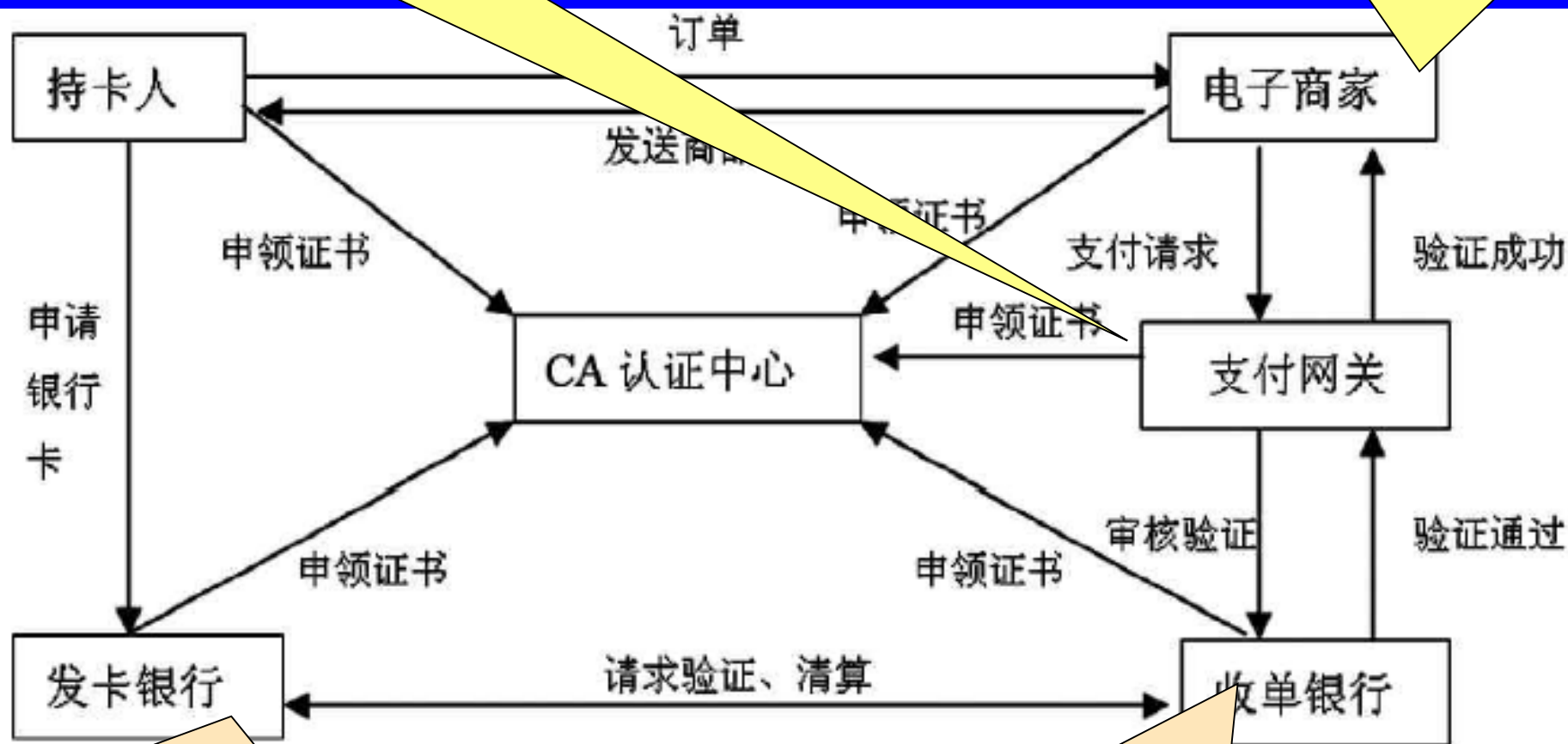
- 信息的机密性
 - 对持卡人的帐户信息和订购信息进行加密，通常用**DES**加密
- 数据的完整性
 - 采用**SHA-1**哈希编码及**RSA**数字签名
 - 采用**SHA-1**的**HMAC**保护
- 持卡人的帐户认证
 - 采用**RSA**数字签名的**X.509v3**证书
- 商家认证
 - 采用**RSA**数字签名的**X.509v3**证书



SET

支付网关：收单行的一个操作设备，用于处理支付卡授权和支付

商家：出售商品或服务的个人或机构，通常通过WEB网页或电子邮件进行出售。商家还必须和收单行达成协议，保证可以接受支付卡付款。



发卡行：一个金融机构，为持卡人建立一个帐户并发行支付卡，一个发卡行保证对经过授权的交易进行付款。

收单行：一个金融机构，为商家建立一个帐户并处理支付卡授权和支付。



IPSec

- **IP层的安全包括了3个功能域：鉴别、机密性和密钥管理**
- **IPSec的重要概念**
- **鉴别报头(AH), 封装安全有效负载(ESP), 传输模式, 隧道模式, 安全关联(SA), 安全关联组(SA Bundle), ISAKMP.**
- **IPSec, IPv6将使互联网(尤其是网络安全)发生巨大变化**



VPN实现原理与方案

- **VPN**是一种架构在公用通信基础设施上的专用数据通信网络，利用**IPSec**等网络层安全协议和建立在**PKI**上的加密与签名技术来获得私有性。
- **IPSec**



实现VPN的关键技术

- 实现VPN的关键技术有：
- 隧道化协议（**Tunneling Protocol**）

隧道技术是将分组封装（**Capsule**）的技术，它是VPN实现以内部网地址通信与多协议通信的重要功能，PPTP、L2TP、IPSec、GRE和GTP被广泛采用。

- 认证协议

在远程访问VPN中，使用了用户名及口令，它们被用来判断用户名是否有权访问。PPP采用了PAP（**Password Authentication Protocol**）及CHAP（**Challenge Handshake Authentication Protocol**）等规程进行认证。PPTP及L2TP等隧道协议采用这种PPP的认证协议。

- 加密技术

加密技术由IPSec ESP（**Encapsulating Security Payload**）。



相关资料



PKI实现(open source)

- OpenCA Project (<http://www.openca.org/>)
- OSCAR PKI Project (<http://oscar.dstc.qut.edu.au/>)
- Jonah PKIX (<http://web.mit.edu/pfl/>)
- pyCA (<http://www.pyca.de/>)
- Mozilla Open Source PKI Project (<http://www.mozilla.org/projects/security/pki/>)



密码算法Toolkit

- **OpenSSL Project (Open Source)**
 - <http://www.openssl.org/>
- **CDSA (Open Source)**
 - <http://developer.intel.com/ial/security/>
- **RSA BSAFE (Commercial Version)**
 - <http://www.rsasecurity.com/products/bsafe/index.html>



Thank You!

