

9.PKI（Public Key infrastructure）

- **PKI相关标准团体**
  - **IETF的X.509 Working Group**（**PKIX** Public Key Infrastructure on X.509）
  - **RSA安全实验室的PKCS**（**Public Key Cryptography Standards**）

“A public key infrastructure (PKI) consists of protocols, services, and standards supporting applications of public key cryptography.”

--RSA FAQ



数字证书的作用

- 公钥的真实性如何保证？
- 数字证书（**Digital Certificate**）提供一种在Internet上验证身份的方式，是用来标志和证明网络通信双方身份的数字信息文件。
  - 使公钥系统得以提供认证、数据完整性、机密性和不可否认等安全服务



数字证书的作用

- 数字证书是由权威公正的第三方机构即CA中心签发的。它是在证书申请被认证中心批准后，通过登记服务机构将其发放给申请者。
- 1996年 X.509 v3, 2000年X.509 v4
- X.509 v4中引入了公钥证书扩展项，可在证书结构中保存任何类型的附加数据以实现用户自定义的安全策略或标识用户属性，从而提供比身份信息更为重要的权限或者属性信息

数字证书的内容

- 最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。一般情况下证书中还包括密钥的有效时间，发证机关(证书授权中心)的名称，该证书的序列号等信息，证书的格式遵循ITU-T X.509国际标准。
- 一个标准的X.509数字安全证书包含以下一些内容：
  - （1）证书的版本号。不同的版本的证书格式也不同，在读取证书时首先需要检查版本号。
  - （2）证书的序列号。每个证书都有一个唯一的证书序列号。
  - （3）证书所使用的签名算法标识符。签名算法标识符表明数字签名所采用的算法以及使用的参数。
  - （4）证书的发行机构名称。创建并签署证书的CA的名称，命名规则一般采用X.500格式。
  - （5）证书的有效期。证书的有效期由证书有效起始时间和终止时间来定义。
  - （6）证书所有人的名称。命名规则一般采用X.500格式；
  - （7）证书所有人的公开密钥及相关参数。相关参数包括加密算法的标识符及参数等
  - （8）证书发行机构ID。这是版本2中增加的可选字段。
  - （9）证书所有人ID。这是版本2中增加的可选字段。
  - （10）扩展域。这是版本3中增加的字段，它是一个包含若干扩展字段的集合。
  - （11）证书发行机构对证书的签名，即CA对证书内除本签名字段以外的所有字段的数字签名。

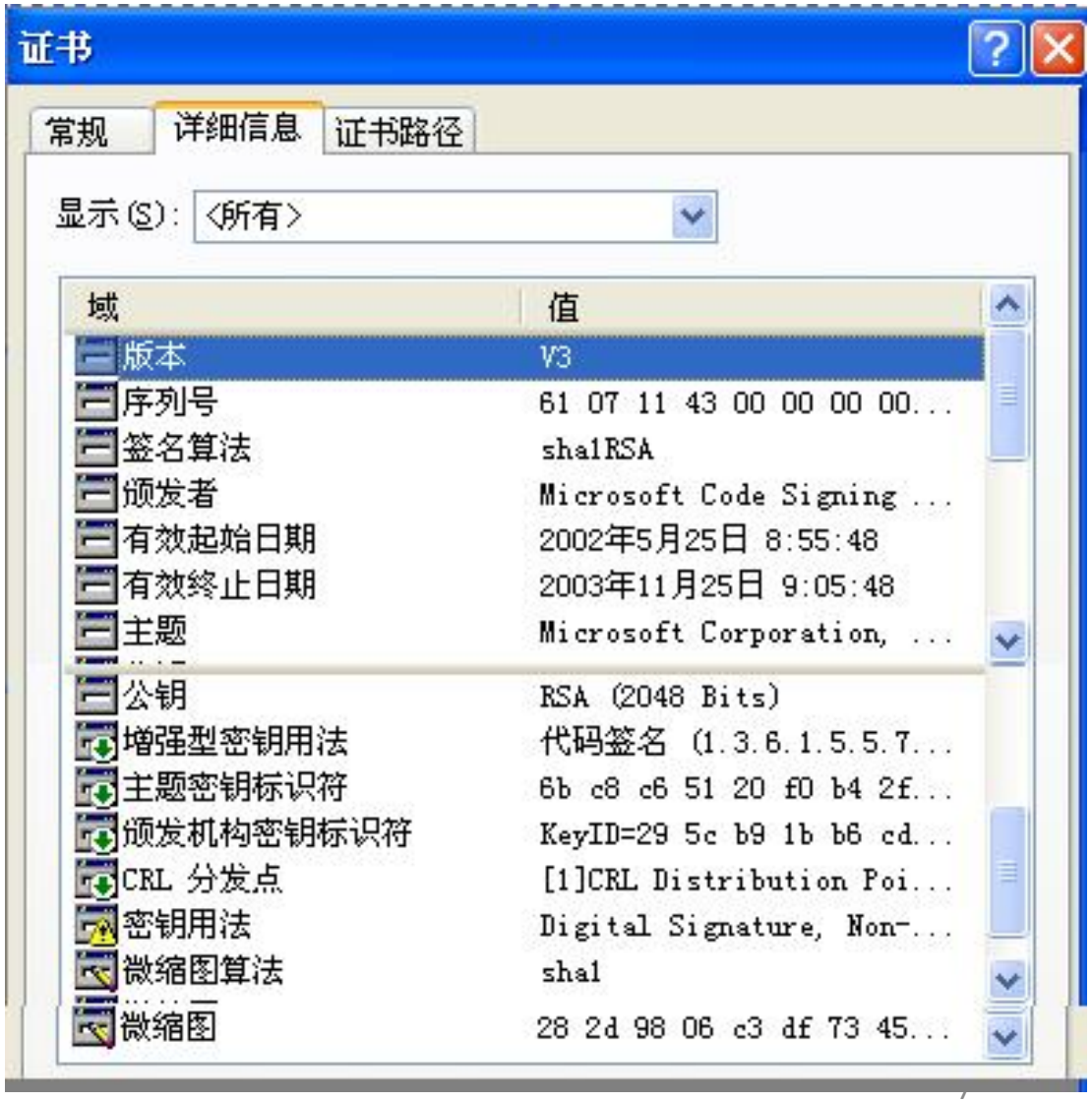
其它证书：简单PKI证书，PGP证书，属性证书

用户可以创建自己的PGP证书，但是必须向CA请求才能得到一份X.509证书。

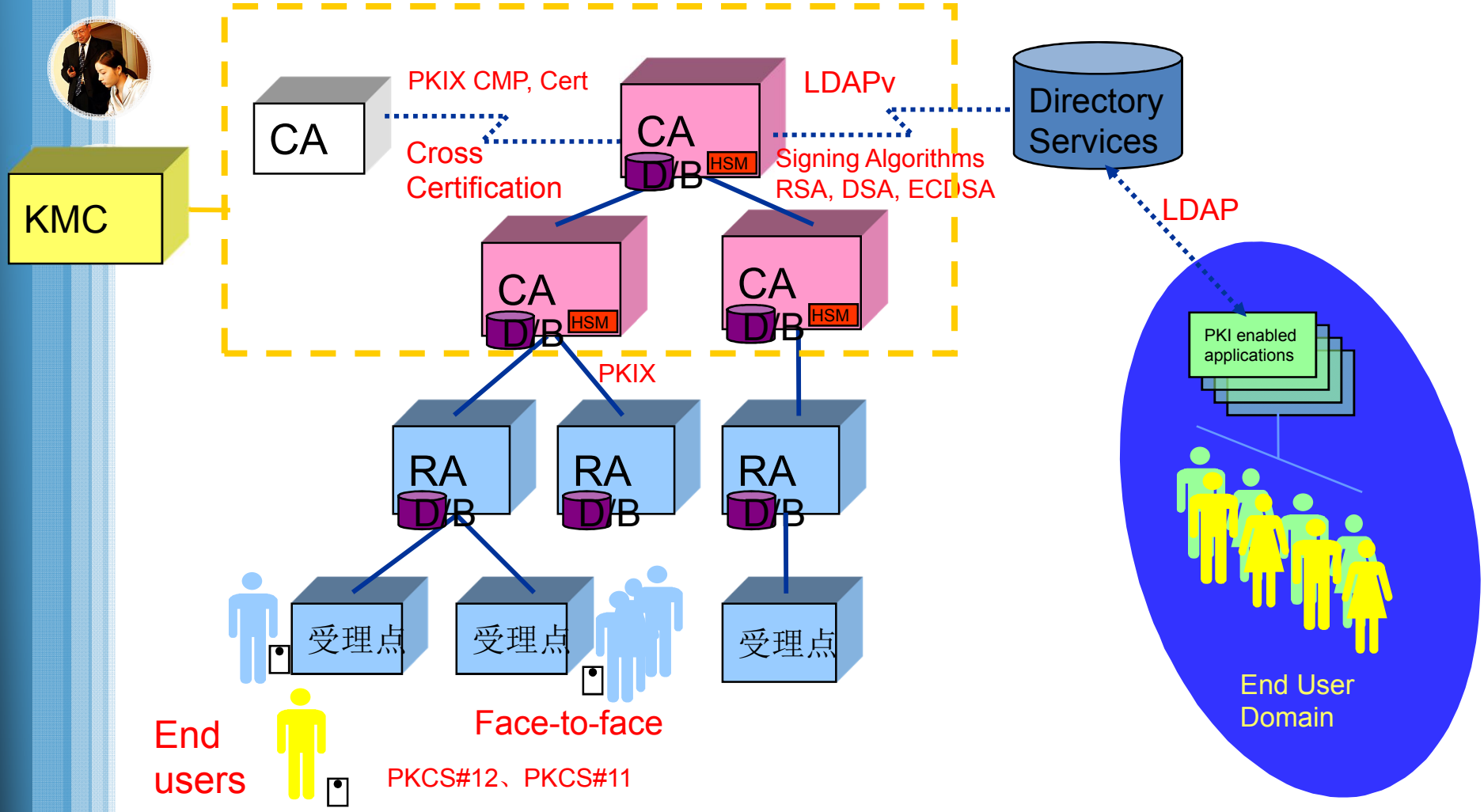


数字证书格式（X.509）

- 证书的版本号
- 数字证书的序列号
- 证书拥有者的姓名
- 证书拥有者的公开密钥
- 公开密钥的有效期
- 签名算法
- 颁发数字证书的验证



PKI系统标准结构


CA
PKIX CMP, Cert
Cross
Certification
CA
D/B
HSM
LDAPv
Signing Algorithms
RSA, DSA, ECDSA
Directory
Services
KMC
CA
D/B
HSM
CA
D/B
HSM
LDAP
PKIX
PKI enabled
applications
RA
D/B
RA
D/B
RA
D/B
受理点
受理点
受理点
End User
Domain
End
users
Face-to-face
PKCS#12、PKCS#11



Certification Authority(CA)
证书机构

- A Certification Authority is a trusted agency that can issue digital certificate

证书机构就是可以签发数字证书的信任机构

- Generally a CA is a reputed organization

通常证书机构是一个著名的组织，如 **Verisign** and **Entrust**



Certification Authority(CA)of China

中国的证书机构,例：

中国金融认证中心（CFCA)
www.cfca.com.cn

北京数字证书认证中心
http://www.bjca.org.cn

广东省电子商务认证中心
http: //www.cnca.net

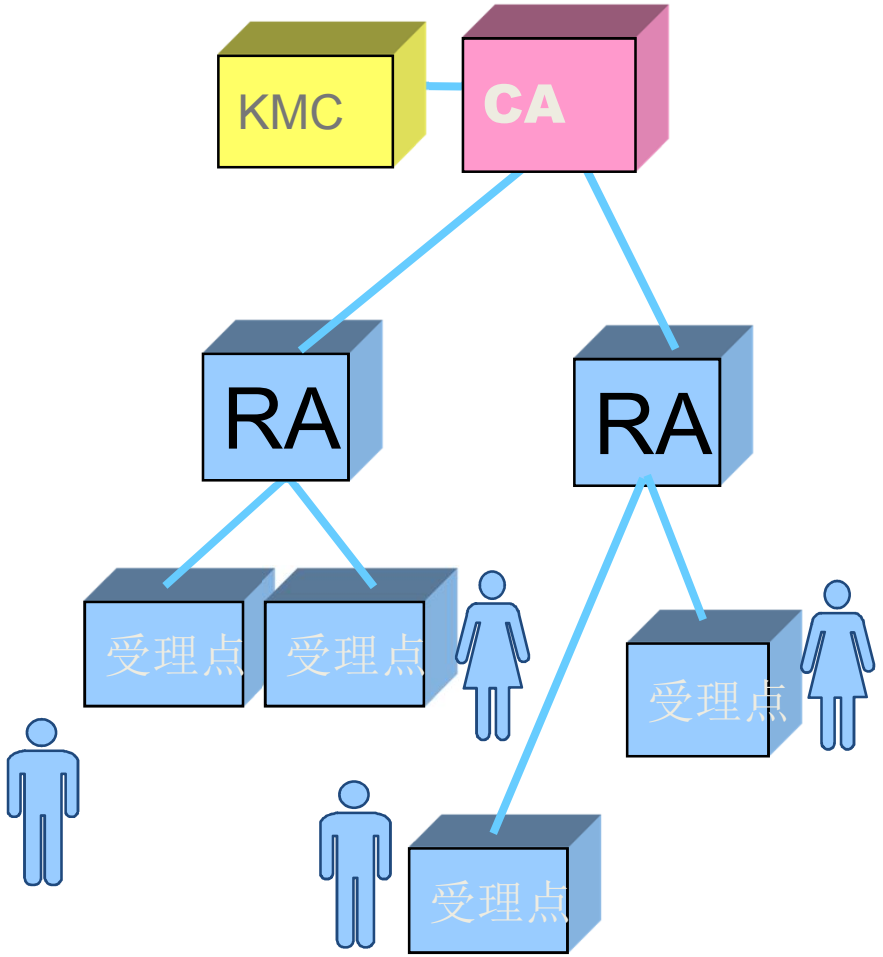
黑龙江邮政局电子邮政安全认证中心
www.e-tol.com.cn

北京国富安电子商务安全认证中心
www.cacenter.com.cn



Registration Authority - RA

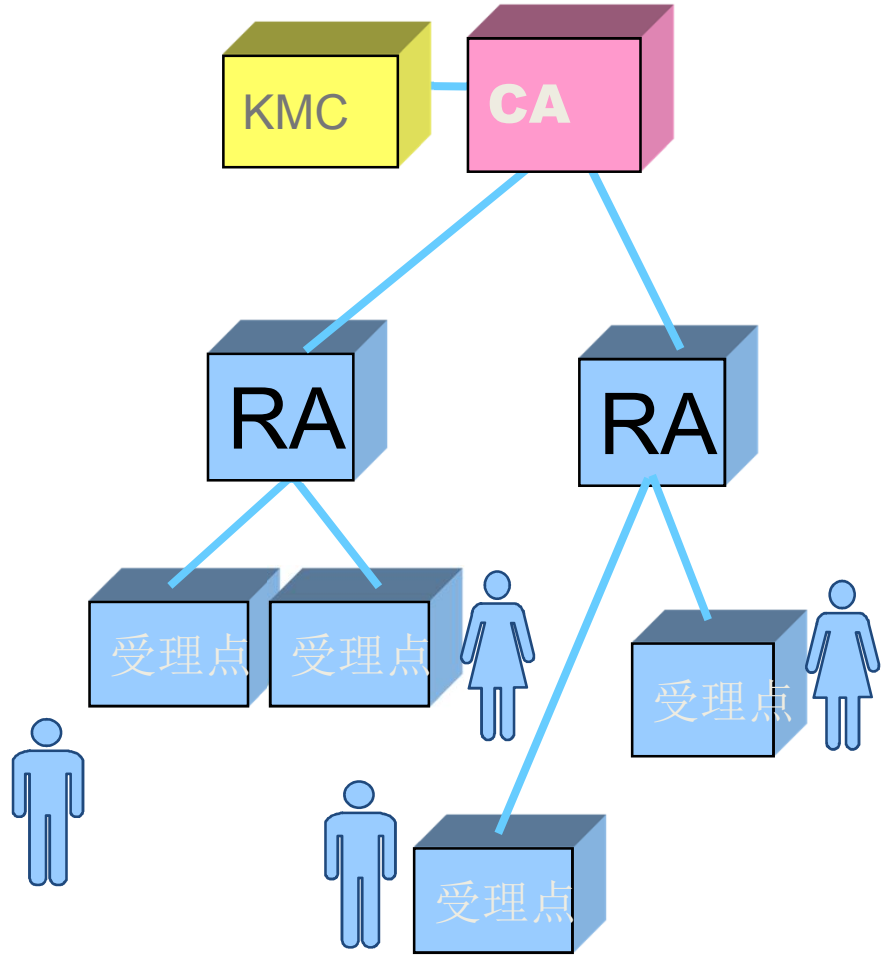
- 进行用户身份信息的审核，确保其真实性；
- 本区域用户身份信息管理和维护；
- 数字证书的下载；
- 数字证书的发放和管理。





证书受理点 - RA 操作端

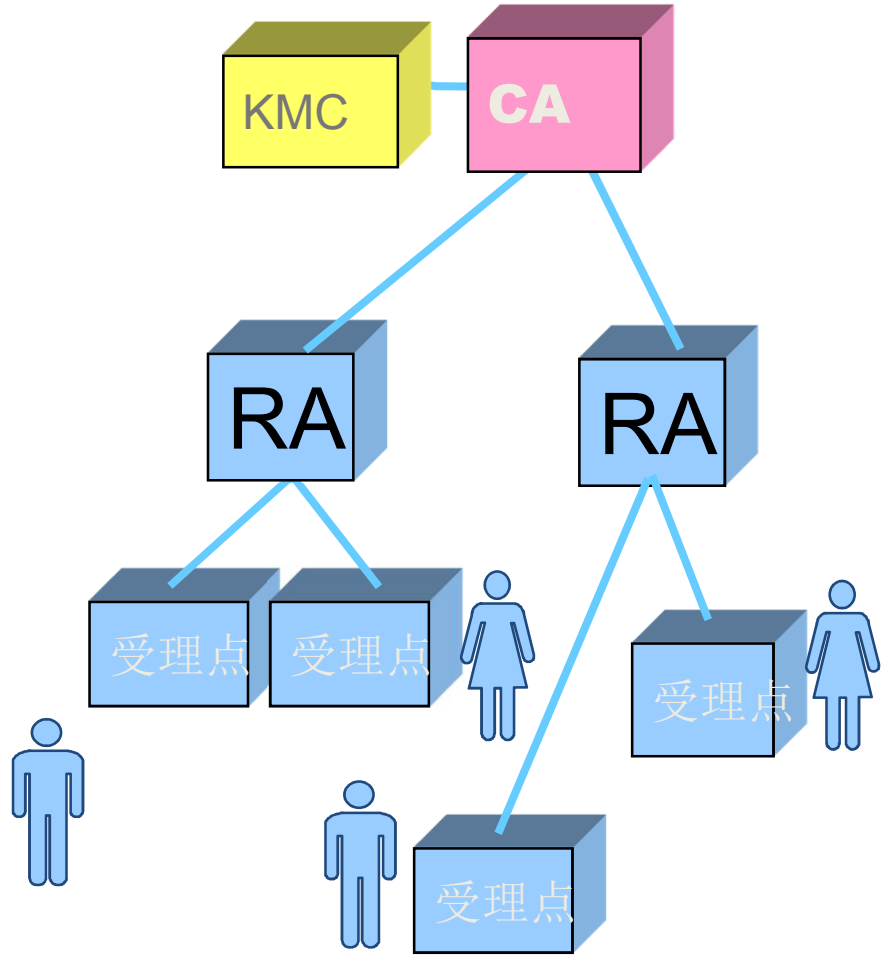
- 收集和管理申报材料和信息
- 录入身份信息
- 初步审核与提交身份信息
- 制作数字证书
- 发放数字证书





密钥管理中心 - KMC

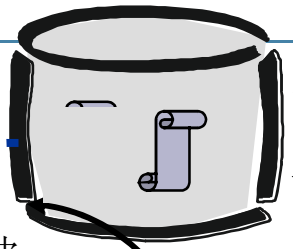
- 密钥的生成
- 密钥的分发
- 密钥的备份
- 密钥的恢复
- 密钥的更新
- 密钥的归档
- 密钥查询
- 密钥销毁





PKI系统如何工作

Directory



Applications and other users

审核通过的注册请求发送给CA

证书同时要被发布出去

CA为用户签发证书

下载凭证

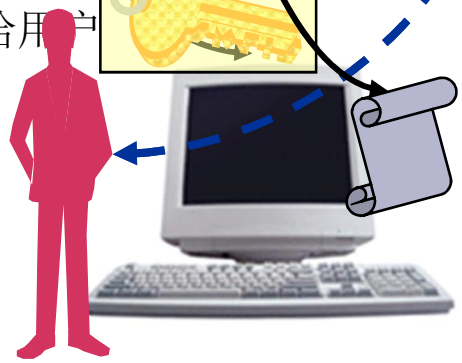
提交证书申请请求

证书下载到用户本地

RA系统审核用户身份

RA将证书载凭证发给用户

发送注册信息给RA



一个新用户申请证书

应用程序通过证书：

- 获取用户的身份信息
- 进行证书废止检查
- 检查证书的有效期
- 校验数字证书
- 解密数据

使用数字证书的用户之间通过CA（一个可信的第三方）来建立信任关系



证书管理协议（CMP）

- 常用的证书管理协议
  - **PKCS** (Public-Key Cryptography Standards)
  - **CMP (Certificate Management Protocol)**
  - **CMC (Certificate Management Messages)**
  - **SCEP (Simple Certificate Enrollment Protocol)**
  - **IETF OCSP (Online Certificate Status Protocol)**



公钥密码标准PKCS (Public-Key Cryptography Standards)

- 公钥密码标准PKCS是由RSA实验室与其它安全系统开发商为促进公钥密码的发展而制订的一系列标准，是最早的公钥密码标准，也是公钥密码发展过程中最重要的标准之一。
- 许多正式和非正式工业标准部分内容的制订都参照了PKCS，如ANSI X9, PKIX, SET, S/MIME, 和SSL等
- PKCS标准提供了基本的数据格式定义和算法定义，它们实际是今天所有PKI实现的基础。



公钥密码标准PKCS

- PKCS #1: RSA Cryptography Standard RSA密码标准
- PKCS #2和PKCS #4：已并入1。
- PKCS #3: Diffie-Hellman Key Agreement Standard DH密钥交换标准
- PKCS #5: Password-Based Cryptography Standard基于口令的密码标准
- PKCS #6: Extended-Certificate Syntax Standard证书扩展语法标准，规定了使用一组属性来扩展X.509证书的句法
- **PKCS #7**: Cryptographic Message Syntax Standard加密消息语法标准PKCS#7为使用密码算法的数据规定了通用语法，比如：邮件和数字签名和数字信封如何封装。
- PKCS #8: Private-Key Information Syntax Standard私钥信息语法标准
- PKCS #9: Selected Attribute Types可选属性类型



例： PKCS7

- pkcs7包括6种数据内容：数据(data),签名数据（sign），数字信封数据（enveloped），签名数字信封数据（signed_and_enveloped），摘要数据（digest），加密数据（encrypted）。

签名数据（sign）：包括签名者的证书，CRL等，目的为确定发送者的身份。
type为NID_pkcs7_signed。PKCS7_SIGNED类型的数据，定义如下:

```
typedef struct pkcs7_signed_st
{
ASN1_INTEGER *version; /* version 1 */ //版本
STACK_OF(X509_ALGOR) *md_algs; /* md used */ //摘要算法
STACK_OF(X509) *cert; /* [ 0 ] */ //签名证书
STACK_OF(X509_CRL) *crl; /* [ 1 ] */ //证书吊销列表
STACK_OF(PKCS7_SIGNER_INFO) *signer_info;   签名信息
struct pkcs7_st *contents;
} PKCS7_SIGNED;
```



- PKCS #10: Certification Request Syntax Standard证书请求语法标准
- PKCS #11: Cryptographic Token Interface Standard密码令牌接口标准
- PKCS #12: Personal Information Exchange Syntax Standard个人信息交换语法标准 ：**存储或传输密钥和证书的安全格式**（.pfx文件）
- PKCS #13: Elliptic Curve Cryptography Standard椭圆曲线密码标准
- PKCS #14: Random Number Generation Standards （伪随机数生成标准）
- PKCS #15: Cryptographic Token Information Format Standard密码令牌信息格式



标准	PKCS #											其它标准
	1	3	5	6	7	8	9	10	11	12	15	
自由算法语法：												
数字签名信息					x		x					
数字信封加密信息					x							
认证请求							x	x				
数字证书												X.509, RFC 1422
扩展证书				x			x					
证书撤销列表												X.509, RFC 1422
私钥加密信息						x	x					
密码令牌									x		x	
个人交换信息										x		
密钥交换信息												[ISO90a], [ISO90b]
特定算法语法：												
RSA 公钥	x											
RSA 私钥	x											
算法：												
消息摘要：MD2, 5												RFCs 1319, 1321
私钥加密：DES												RFC 1423, [NIST92a]
公钥加密：RSA	x											
签名：MD2,4,5w/RSA	x											
基于口令的加密			x									
D-H 密钥交换		x										



CMP (Certificate Management Protocol)

- 1999年， RFC 2510和RFC 2511
- PKIX工作组在上面两个标准的基础上开放了CMP
- CMP在处理证书的请求和响应消息方面可代替PKCS
- CMP协议支持许多不同的证书管理功能



CMC（Certificate Management Messages)

- RFC2797，PKIX工作组为了代替CMP而发布了CMC
- CMC使用PKCS#10处理证书请求消息
- CMC使用PKCS#7处理证书的响应消息
- CMC引用RFC 2511来支持由CMP定义的更高级的证书请求格式
- CMC总体目标是在保持简洁性的同时提供高级证书管理功能，并支持广泛使用的PKCS



SCEP

- **SCEP，Simple Certificate Enrollment Protocol，简单证书登记协议**
- **Cisco公司开发**
- **网络设备的证书登记协议**
- **采用PKCS#10和PKCS#7来支持证书的请求和响应消息**
- **SCEP支持CRL和网络设备作出的证书询问**
- **SCEP不是完整的证书管理协议**



证书吊销

- CA在证书过期之前使证书失效
- CA需要两种方法来吊销证书并通知吊销的终端实体
  - CRL（ Certificate Revocation List）
  - OCSP



CRL

- **CRL，Certificate Revocation List，证书吊销列表**
- **RFC 2459定义了X.509v2 CRL的格式**
- **CRL的数据结构类似于证书**
- **证书被吊销后，CA会将该证书加入吊销列表，然后发行的CA对数据结构签发数字签名，从而创建一个有效的X.509 CRL**



CRLCRL（续）

—— X.509 CRL的内容

版本	所表示的CRL版本
签名（Signature）	CA签发CRL所用的数字签名算法
发行者（Issuer）	发行机构的名字
此次更新（ThisUpdate）	CRL的发布时间
下次更新（NextUpdate）	发布下个CRL的时间
被吊销的证书（RevokedCertificate）	按序列号吊销的证书的列表
CRL扩展（crlExtensions）	CRL版本2的可选项
下面是CA的数字签名（Digital Signature of CA below）	
签名算法（SignatureAlgorithm）	CA签发证书所使用的数字签名算法
签名值（SignatureValue）	CA创建的实际数字签名



Logical View of a CRL

CRL的逻辑视图

CA: XYZ
Certificate Revocation List (CRL)
This CRL: 1 Jan 2002, 10:00 am
Next CRL: 12 Jan 2002, 10:00 am

Serial Number	Date	Reason
1234567	30-Dec-01	Private key compromised
2819281	30-Dec-01	Changed job
……		

Fig 5.27

Example



Delta CRL
差异CRL

- Reduces the burden of a full CRL

  减小完全CRL的负担
- Contains list of revoked certificates since the last CRL was issued

  包含自最近发布的CRL以来的证书吊销列表
- Better performance

  较优的性能

Delta CRL
差异CRL

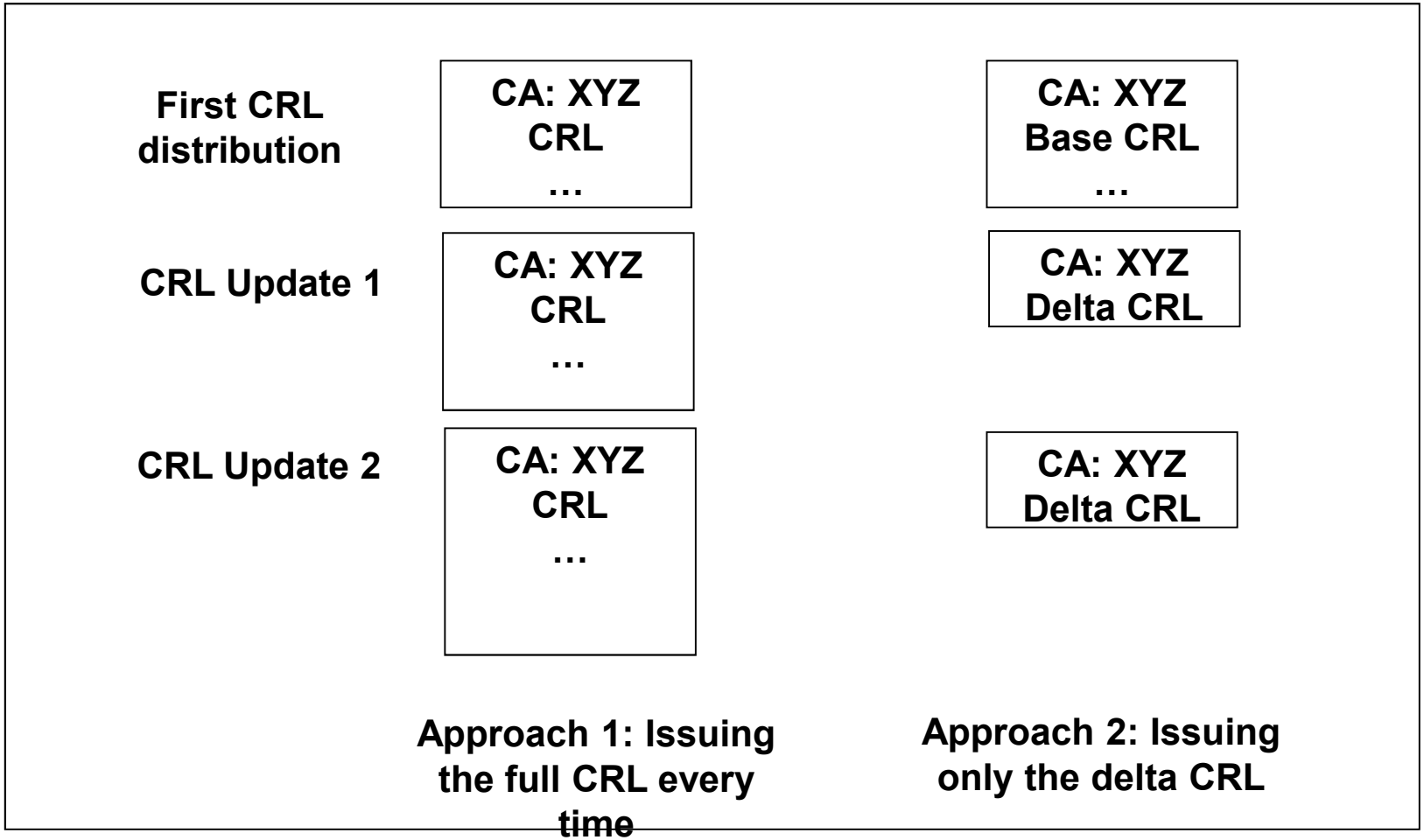


Fig 5.29



CRL（续）

- CA将CRL公布于一个公共存储库，终端实体都可以对该存储库进行检索
- 主体在收到一个证书时，首先检索CRL，判断这个证书是否是有效的
- 使用CRL最大的困难是缩短证书吊销和终端实体知道该消息之间的时间间隔



OCSP

- **IETF OCSP， Online Certificate Status Protocol，**在线证书状态协议
- 实时证书吊销检查机制,为PKI用户提供一条方便快捷的数字证书状态查询 通道
- 终端实体同**OCSP**响应程序之间的消息必须是安全的



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

- Request-Response Model

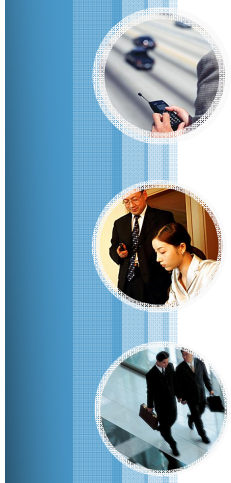
  请求-响应模式

- Client sends OCSP Request (Is a certificate valid?)

  客户发送**OCSP**请求（证书有效吗？）

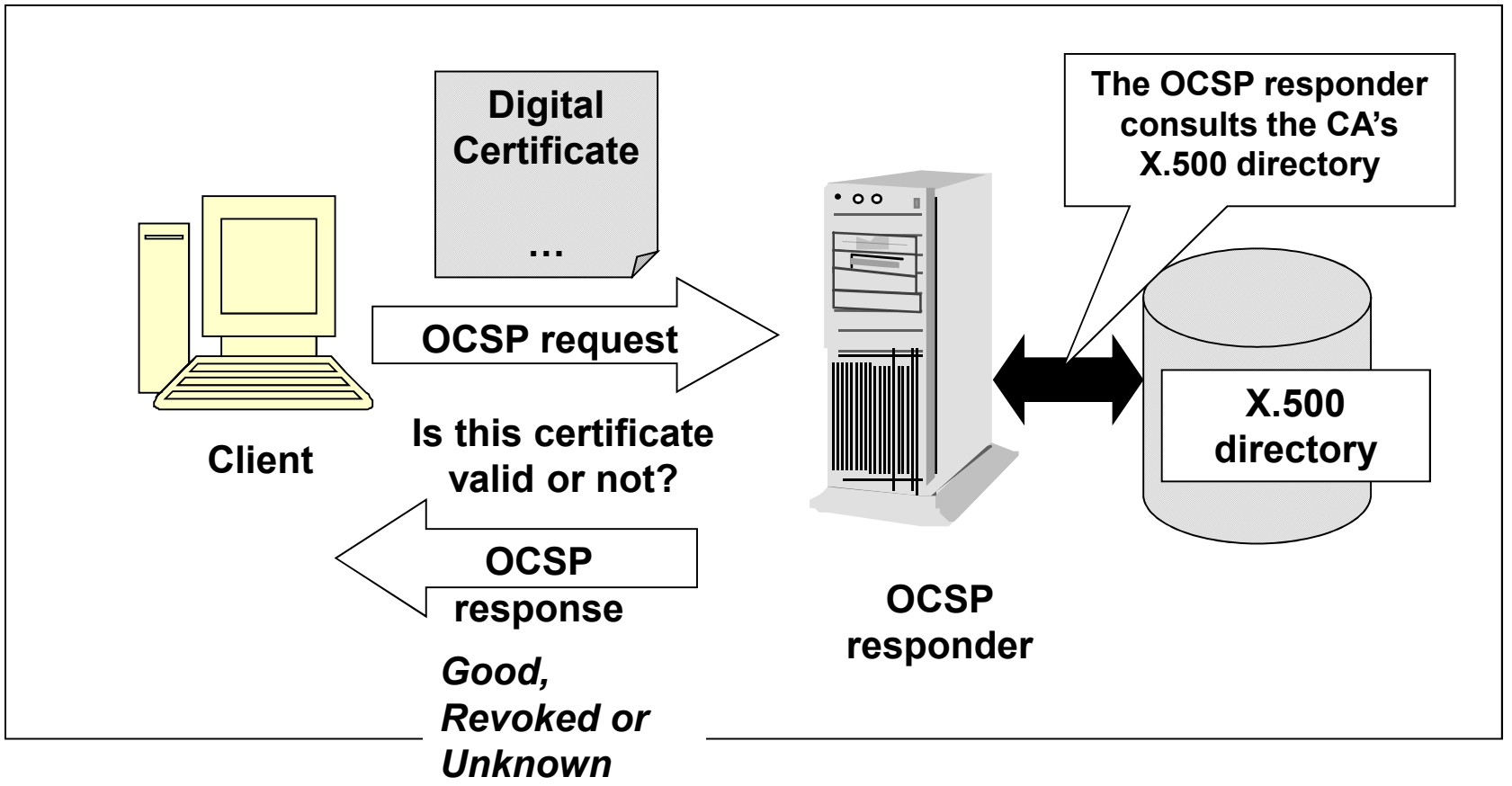
- Server sends OCSP Response (The certificate is valid/invalid/not sure)

  服务器发送**OCSP**响应（证书有效/无效/不确定）



OCSP Response

OCSP响应



XKMS（XML Key Management Specification）

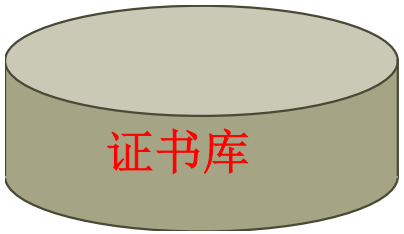


- 由VeriSign、Microsoft和webMethods三家公司在W3C共同推动的公钥配置与注册规范，它为访问和集成PKI拟出了一种便捷规范的机制，以简化公钥的注册、管理和查询服务，减少客户端应用程序设置的复杂性，降低与PKI建立信任关系的复杂度。
- XKMS由两种服务组成：
  - X-KISS，XML Key Information Service Specification:公钥的定位和查询等服务
  - X-KRSS，XML Key Registration Service Specification公钥的注册



证书存储库

- 证书存储库用于存储、分发证书和**CRL**
- 在应用规模较大时，需要使用证书库
- 证书存储库可由所有终端实体和**CA**访问
- 可以使用的技术
  - 目录服务
  - **LDAP**
  - **FTP** 和 **HTTP**





证书存储库(续)
—— 目录服务和LDAP

- 目录服务（**Directory Service**）：在线存储库
- 目录服务包含对象的有关信息
- **RFC 2587**定义了支持**PKI**的目录中所使用的对象类和属性
- **LDAP，Lightweight Directory Access Protocol**，轻量级目录访问协议，用于访问目录中的信息，同目录交互。LDAP v3已经在PKI体系中被广泛应用于证书信息发布、CRL信息发布、CA政策以及与信息发布相关的各个方面。



时间戳颁发机构（TSA）

- PKI可以提供保密性、来源认证和数据完整性、不可否认服务
- 为了更好提供不可否认服务，需要时间戳服务
- RFC 2001描述了TSA的使用方式

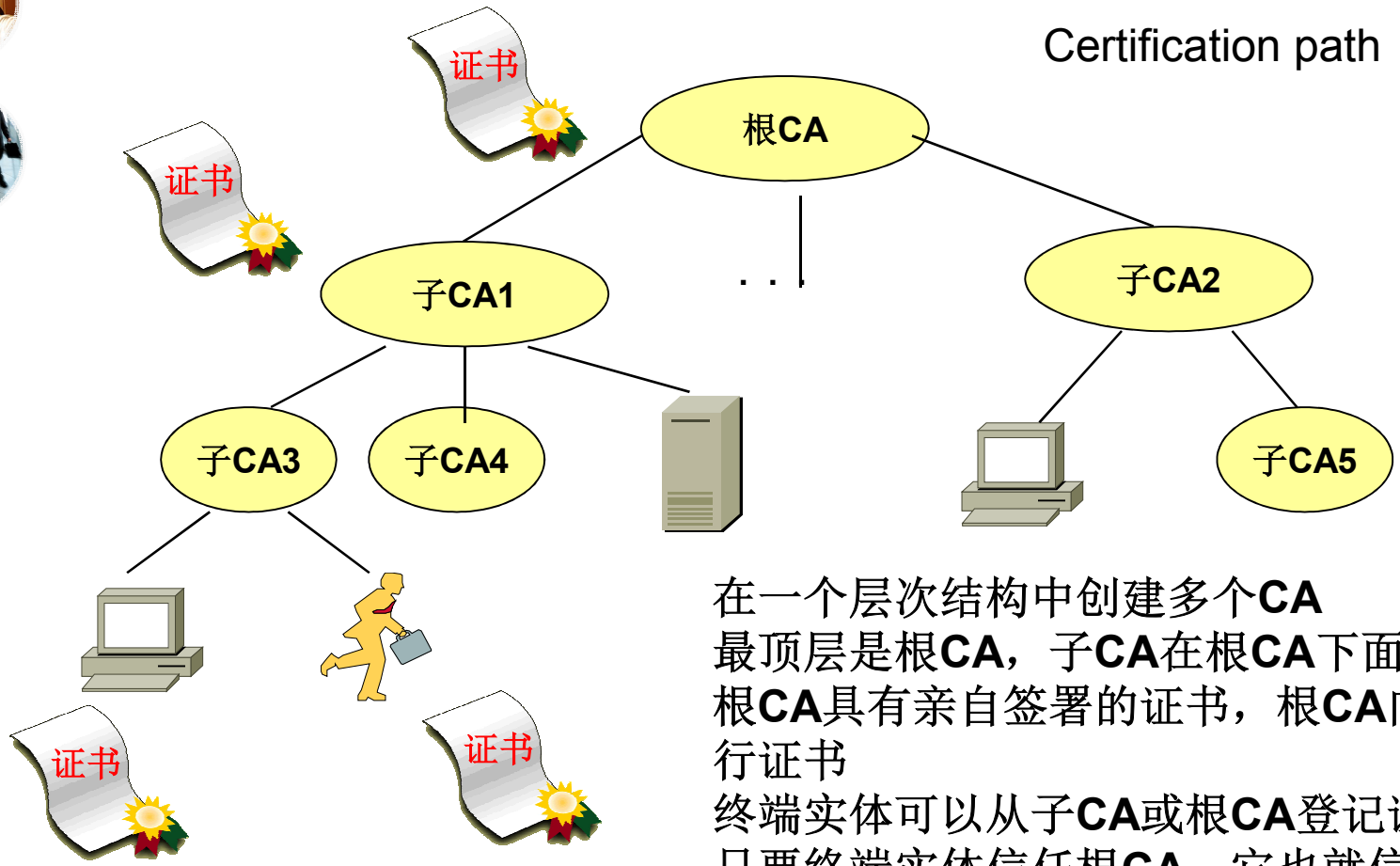


PKI体系结构

- **PKI系统中可以包含多个CA**
- 使用的技术
  - 层次结构模型
  - 交叉证明
  - 混合模型



层次结构模型

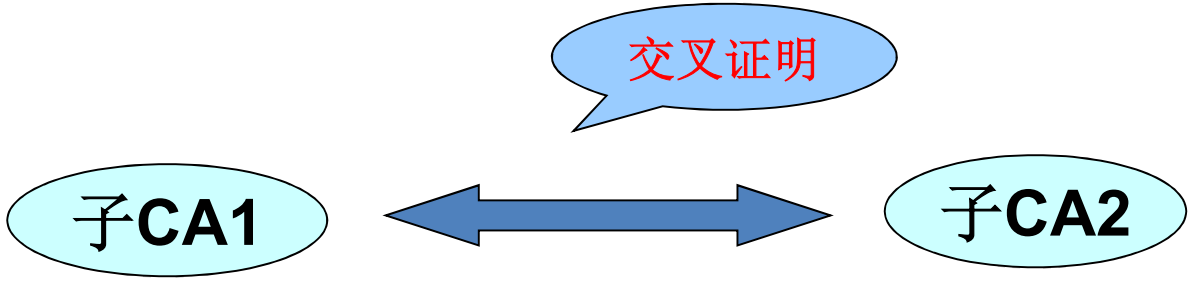


在一个层次结构中创建多个CA
最顶层是根CA，子CA在根CA下面
根CA具有亲自签署的证书，根CA向子CA发行证书
终端实体可以从子CA或根CA登记证书
只要终端实体信任根CA，它也就信任子CA
终端实体可以从某个子CA及其同等逻辑层次上的CA上检索证书



交叉证明

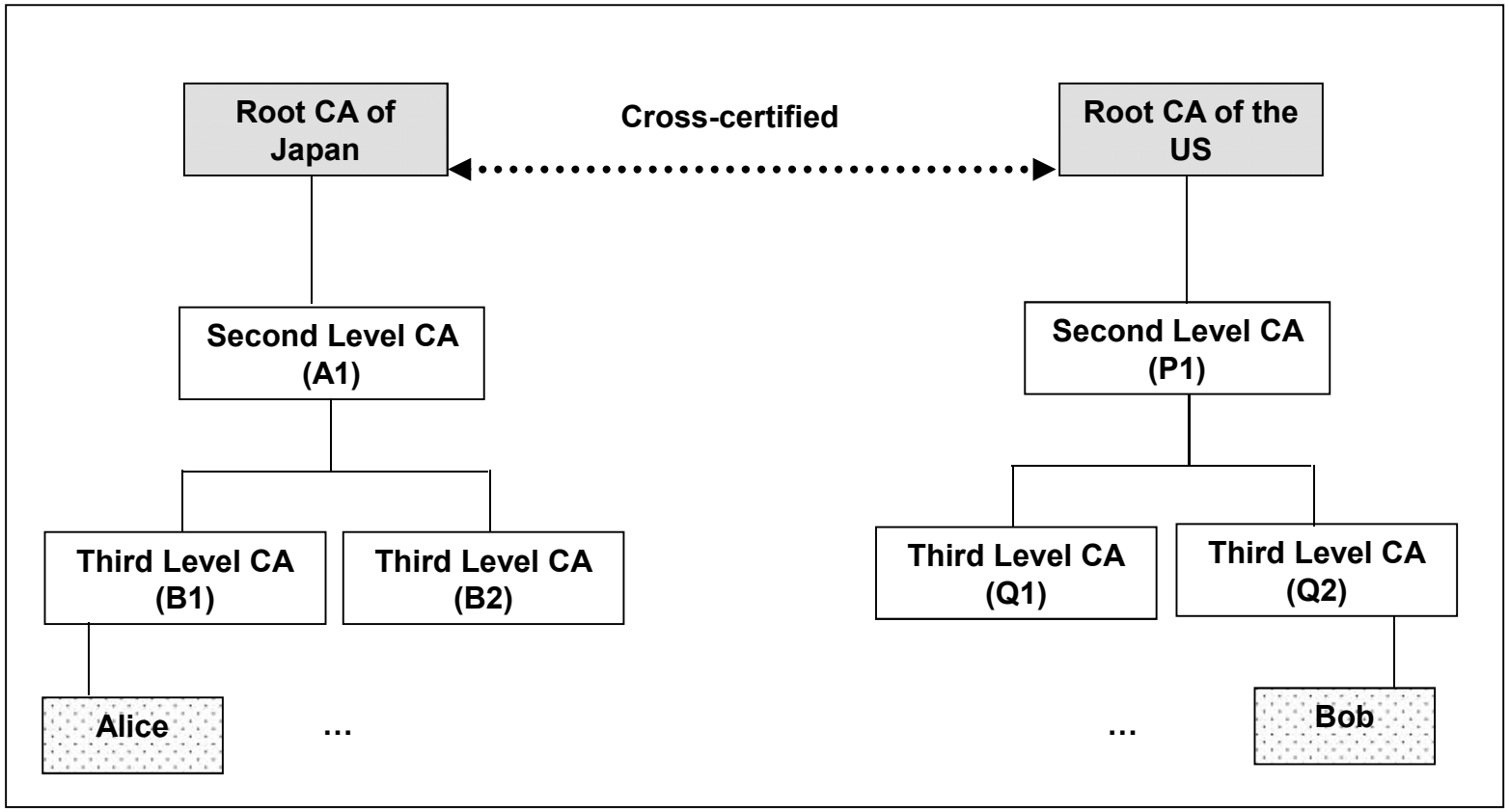
- 交叉证明指CA之间互相证明以建立一种横向信任关系，这是一种对等信任模型
- 交叉证明为不同PKI实现相互集成提供了方便途径





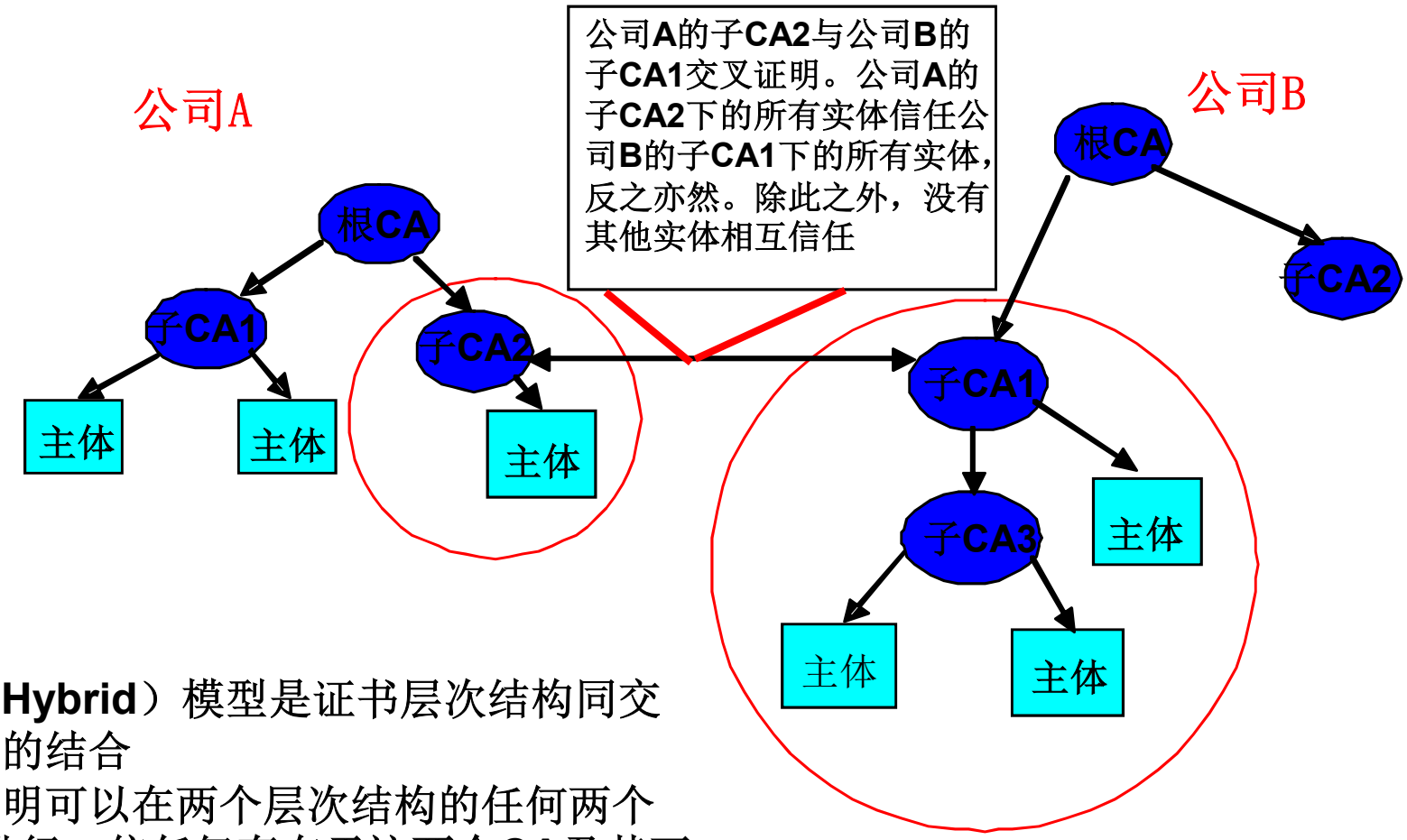
Cross-Certification of Cas

CA的交叉证书





混合模型



混合（**Hybrid**）模型是证书层次结构同交叉证明的结合

交叉证明可以在两个层次结构的任何两个**CA**间进行，信任仅存在于这两个**CA**及其下面的子**CA**之间



PMI授权管理基础设施

- PMI（Privilege Management Infrastructure，授权管理基础设施）是NISI（National Information Security Infrastructure，国家信息安全基础设施）的一个重要组成部分。
- 建立在PKI基础上的PMI，以向用户和应用程序提供权限管理和授权服务为目标
- X.509v4提出了属性证书，可作为X.509身份证书的扩展或单独的属性证书。
- PMI实际提出了一个新的信息保护基础设施，能够与PKI和目录服务紧密地集成，并系统地建立起对认可用户的特定授权，对权限管理进行了系统的定义和描述，完整地提供了授权服务所需过程
- 主要负责向业务应用系统提供与应用相关的授权服务管理，提供用户身份到应用授权的映像功能，实现与实际应用处理模式相对应的、与具体应用系统开发和管理无关的访问控制机制
- 极大地简化了应用中访问控制和权限管理系统的开发与维护，并减少管理成本和降低其复杂性。
- PMI系统主要分为授权管理中心（又称AA中心）和资源管理中心（又称RM中心）两部分。

PMI与PKI的对比

- PMI以资源管理为核心，对资源的访问控制权统一交由授权机构统一处理，即由资源的所有者来进行访问控制。同公钥基础设施PKI相比，两者主要区别在于：
  - PKI证明用户是谁，而PMI证明这个用户有什么权限，能干什么。
  - PMI（授权管理基础设施）需要PKI （公钥基础设施）为其提供身份认证。
- PMI与PKI在结构上是非常相似的。信任的基础都是有关权威机构，由他们决定建立身份认证系统和属性特权机构。
  - 在PKI中，由有关部门建立并管理根CA，下设各级CA、RA和其它机构；
  - 在PMI中，由有关部门建立授权源SOA，下设分布式的AA和其它机构。



x.509 属性证书（Attribute Certificate）

轻量级的数字证书，不包含公钥信息，只包含证书所有人ID、发行证书ID、签名算法、有效期、属性等信息。一般的属性证书的有效期均比较短，这样可以避免公钥证书在处理CRL时的问题。如果属性证书的有效期很短，到了有效期的日期，证书将会自动失效。

属性一般由属性类别和属性值组成，也可以是多个属性类别和属性值的组合。

属性证书利用属性来定义每个证书持有者的 权限、角色等信息。从而可以解决PKI中所面临的问题，对信任进行一定程度的管理

RFC 5755 An Internet Attribute Certificate Profile for Authorization

```
AttributeCertificate :: =SEQUENCE{
        acinfo AttributeCertificate,
        signatureAlgrithm
AlgorithnIdentifier,
        signatureAlgrithmValue
BITSTRING
}
AttributeCertificate Info :: =SEQUENCE{
        version AttCertVersion -- version
is v2,
        holder Holder,
        issuer AttCertIssuer,
        signautre AlgorithnIdentifier,
        serialNumber
CertificateSerialNumber,
        attrCertValidityPeriod
AttCertValidityPeriod,
       attributes SEQUENCE OF Attribute,
        issuerUniqueID UniqueIdentifier
OPTIONAL,
        extensions Extensions OPTIONAL
}
```



SPKI/SDSI

- In SPKI (Simple public key infrastructure) , an authorization grant is made only locally. If you need to grant authorization to someone beyond your locality, then you may (must) delegate that grant through a chain of local relationships.
- SPKI was merged with Simple Distributed Security Infrastructure
- http://world.std.com/~cme/html/spki.html#UPnP



对比项	PKI	SPKI/SDSI
命名属性	全局	本地
应用方向	身份认证	分布式访问控制
权限传递	不能权限传递	可以传递权限
主体	人	公钥
名字-密钥	一一对应	一对一，一对多
证书格式	格式复杂	简单
撤销方式	证书撤销列表	在线测试
CA中心	证书颁发依赖第三方权威CA	自己是CA
构建难度	构建复杂，需要证书库CA中心，RA注册中心	构建简单，不需要书库CA中心，RA注册中心



实验示例

- OPENSSL建立CA
- 为CA产生RSA公私钥，建立自签名证书ca.crt
- 再产生一对公私钥，由CA发证书
- 命令
  - Openssl ca
  - Openssl genrsa
  - Openssl req

由windows的证书管理可以看到证书