

第七章

密钥管理

主要内容

❖ 对称密码体制的密钥管理

- ❧ 密钥分级
- ❧ 密钥生成
- ❧ 密钥的存储与备份
- ❧ 密钥分配
- ❧ 密钥的更新
- ❧ 密钥的终止和销毁

❖ 公钥密码体制的密钥管理

- ❧ 公钥的分配
- ❧ 数字证书
- ❧ X.509证书
- ❧ 公钥基础设施PKI

关于密钥管理

- ❖ 密钥体制的安全应当只取决于密钥的安全，而不取决于对密码算法的保密。因此密钥管理是至关重要的。
- ❖ 历史表明，从密钥管理的途径窃取秘密要比单纯的破译所花的代价要小得多。
- ❖ 密钥管理包括了密钥的产生、存储、分配、组织、使用、更换和销毁等一系列技术问题。
- ❖ 对称密码体制的密钥管理和非对称密码体制的管理是完全不同的。

7.1 对称密码体制的密钥管理

- ❖ 对称密码体制的加密钥等于解密密钥，因此密钥的秘密性、真实性和完整性必须同时保护。这就带来了密钥管理方面的复杂性。对于大型网络系统，由于所需要的密钥种类和数量都很多，因此密钥管理尤其困难。
- ❖ ANSI(美国国家标准学会, American National Standards Institute)颁布了ANSI X9.17金融机构密钥管理标准，为DES、AES等商业密码的应用提供了密钥管理指导。

密钥分级

❖ 密钥分为初级密钥、二级密钥和主密钥。

❖ 初级密钥

- ❧ 用于加解密数据的密钥
- ❧ 初级通信密钥：一个密钥只使用一次，生存周期很短
- ❧ 初级文件密钥：与其所保护的文件有一样长的生存周期
- ❧ 初级密钥不能以明文形式保存

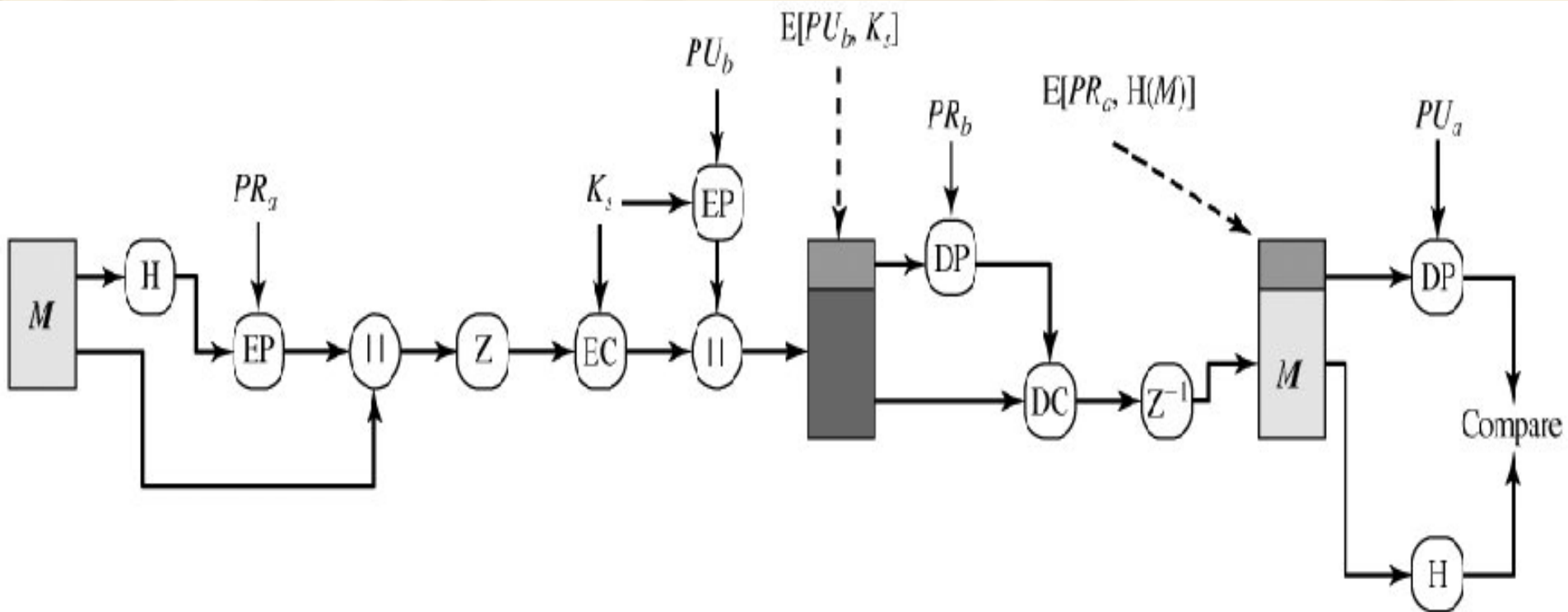
❖ 二级密钥

- ❧ 用于保护初级密钥
- ❧ 不能以明文形式保存

❖ 主密钥

- ❧ 密钥管理方案中的最高级密钥，用于对二级密钥进行保护。主密钥的生存周期很长

PGP系统中的几个密钥



密钥生成

❖ 对密钥的基本要求

- ❧ 具有良好的随机性，包括长周期性、统计意义上的等概率性以及不可预测性等。

❖ 主密钥的产生

- ❧ 用于加解密主密钥应当是高质量的真随机序列,常采用物理噪声源的方法来产生。

❖ 二级密钥的产生

- ❧ 利用真随机数产生器芯片来产生二级密钥
- ❧ 使用主密钥和一个强的密码算法来产生二级密钥

❖ 初级密钥的产生

- ❧ 把随机数视为受高级密钥（主密钥或者二级密钥）加密后的初级密钥。因此，随机数被解密后得到初级密钥。

密钥的存储

- ❖ 安全可靠的存储介质是密钥安全存储的物质条件
- ❖ 安全严密的访问控制机制是密钥安全存储的管理条件。
- ❖ 密钥安全存储的原则是不允许密钥以明文形式出现在密钥管理设备之外。

密钥的存储形态

❖ 明文形态

∞ 密钥以明文形式存储；

❖ 密文形态

∞ 密钥被加密后存储；

❖ 分量形态

∞ 密钥以分量的形式存储，密钥分量不是密钥本身，而是用于产生密钥的部分参数，只有在所有密钥分量共同作用下才能产生出真正的密钥，而且只知道其中一个或部分分量，无法求出其他分量。

密钥的存储

❖ 主密钥的存储

- ❧ 以明文形式存储，存储器必须是高度安全的，不但物理上安全，而且逻辑上安全。通常是将其存储在专用密码装置中。

❖ 二级密钥的存储

- ❧ 通常采用以高级密钥加密的形式存储二级密钥。

❖ 初级密钥的存储

- ❧ 初级文件密钥一般采用密文形式存储，通常采用以二级文件密钥加密的形式存储初级文件密钥。
- ❧ 初级会话密钥的存储空间是工作存储器，应当确保工作存储器的安全。

密钥备份

- ❖ 密钥的备份应当是异设备备份，甚至是异地备份。
- ❖ 备份的密钥应当受到与存储密钥一样的保护
- ❖ 为了减少明文形态的密钥数量，一般采用高级密钥保护低级密钥的方式来进行备份
- ❖ 对于高级密钥，不能以密文形态备份。为了进一步增强安全，可采用多个密钥分量的形态进行备份。
- ❖ 密钥的备份应当方便恢复，密钥的恢复应当经过授权而且要遵循安全的规章制度。
- ❖ 密钥的备份和恢复都要记录日志，并进行审计。

密钥分配

❖ 主密钥的分配

❧ 采取最安全的分配方法。一般采用人工分配主密钥，由专职密钥分配人员分配并由专职安装人员妥善安装。

❖ 二级密钥的分配

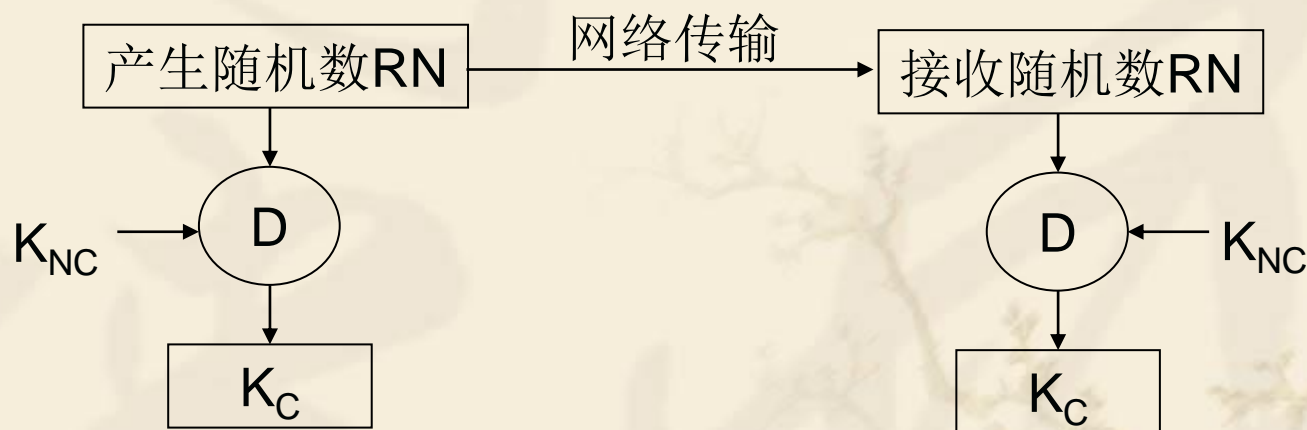
❧ 利用已经分配安装的主密钥对二级密钥进行加密保护，并利用计算机网络自动传输分配。



密钥分配

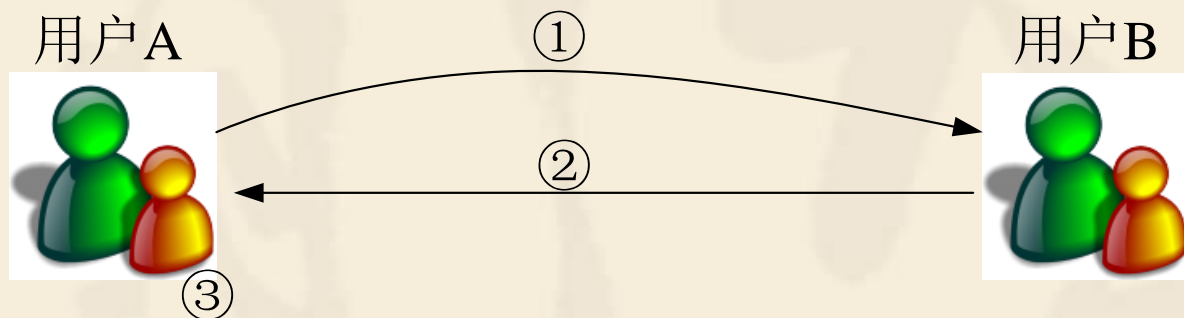
❖ 初级密钥的分配

- 通常总是把一个随机数直接视为一个初级密钥被高级密钥加密之后的结果，这样初级密钥一产生就是密文形式。
- 发送方直接把随机数（密文形式的初级密钥）通过计算机网络传给对方，接收端用高级密钥解密获取初级密钥



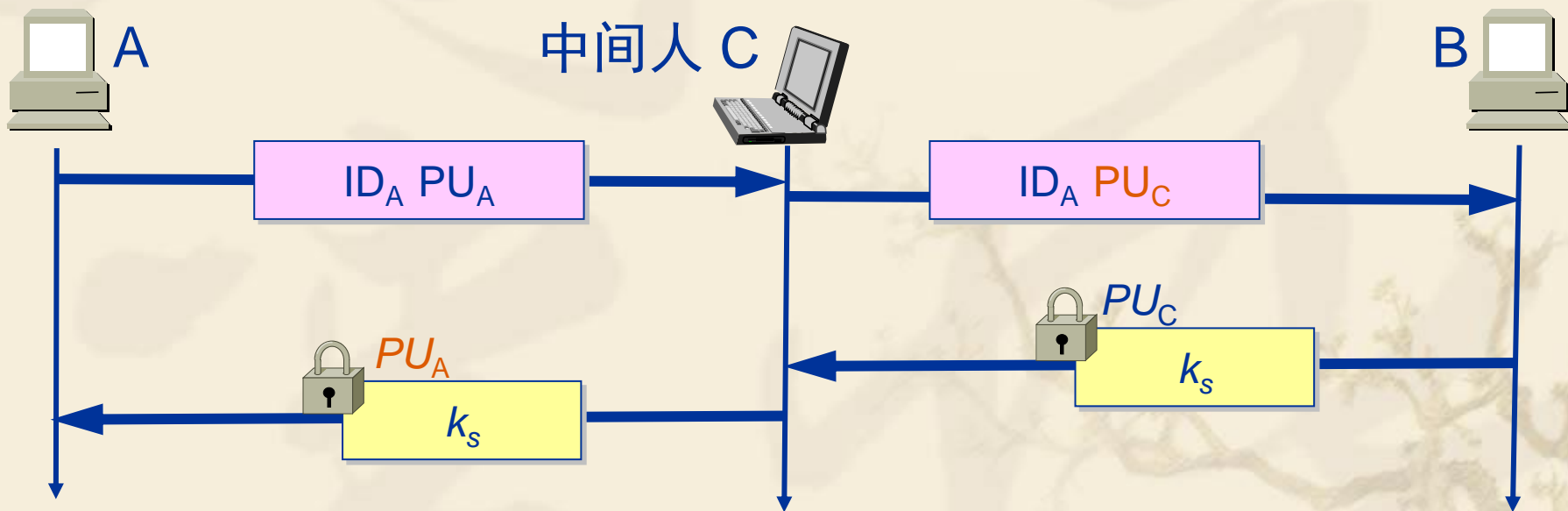
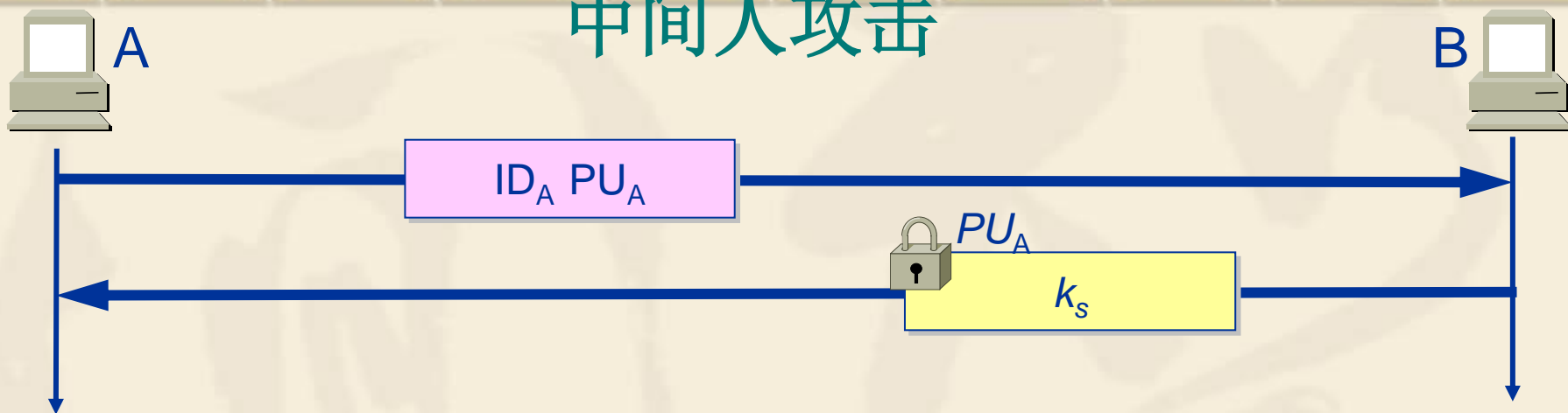
K_{NC} : 二级密钥
 K_C : 初级密钥
RN: 随机数

利用公钥密码体制来分配密钥

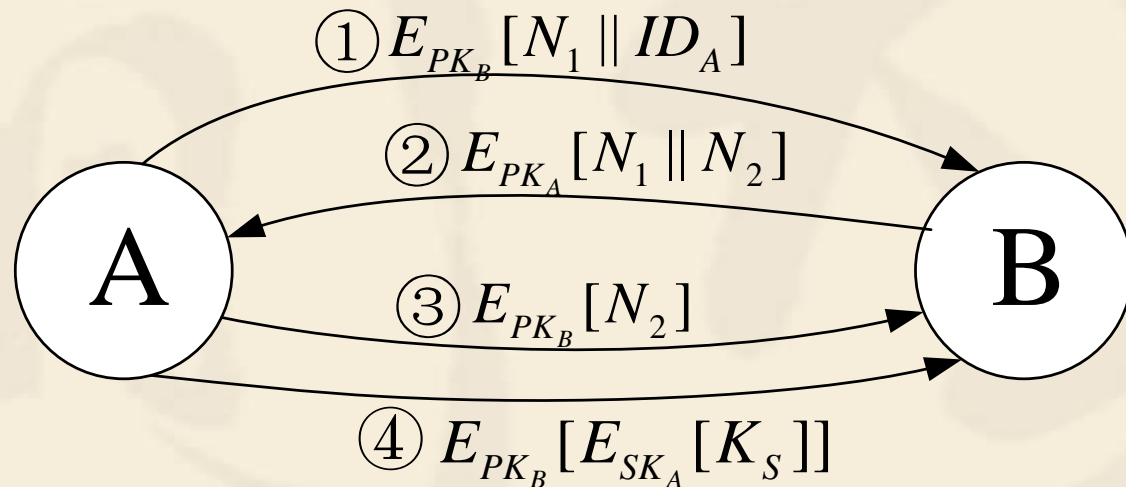


- ① A向B发送自己的公钥和A的身份；
- ② B收到消息后，产生会话密钥 K_s ，用公钥加密后传送给A；
- ③ A用私钥解密后得到 K_s 。

中间人攻击



具有保密性和认证的分配方法



- ① A用B的公钥加密A的身份和一个一次性随机数N1后发送给B；
- ② B解密得到N1，并用A的公钥加密N1和另外一个随机数N2发送给A；
- ③ A用B的公钥加密N2后发送给B；
- ④ A选择一个会话密钥 K_S ，用A的私钥加密后再用B的公钥加密，发送给B，B用A的公钥和B的私钥解密得 K_S 。

密钥的更新

❖ 主密钥的更新

- ❧ 更新时必须重新安装，安全要求与初次安装一样
- ❧ 主密钥的更新将要求受其保护的二级密钥和初级密钥都要更新

❖ 二级密钥的更新

- ❧ 重新产生二级密钥并且妥善安装
- ❧ 受其保护的初级密钥要更新

❖ 初级密钥的更新

- ❧ 初级会话密钥采用“一次一密”的方式工作，所以更新是很容易的。
- ❧ 初级文件密钥更新要麻烦的多，将原来的密文文件解密并且用新的初级文件密钥重新加密。

密钥的终止和销毁

- ❖ 终止使用的密钥并不马上销毁，而需要保留一段时间。这是为了确保受其保护的其他密钥和数据得以妥善处理。只要密钥尚未销毁，就应该妥善保护。
- ❖ 密钥销毁要彻底清除密钥的一切存储形态和相关信息，使重复这一密钥变得不可能。
- ❖ 值得注意的是，要采用妥善的清除存储器的方法，对于磁存储器，简单的删除、清零或写“1”都是不安全的。

7.2 公钥密码体制的密钥管理

- ❖ 公钥密码体制的密钥管理和对称密码体制的密钥管理有着本质的区别。
- ❖ 对称密码体制的密钥本质上是一种随机数或者随机序列，而公钥密码体制本质上是一种单向陷门函数，建立在某一数学难题之上。

Distribution of Public Keys

❖ Several techniques have been proposed for the distribution of public keys. Virtually all these proposals can be grouped into the following general schemes:

❧ Public announcement 公开发布

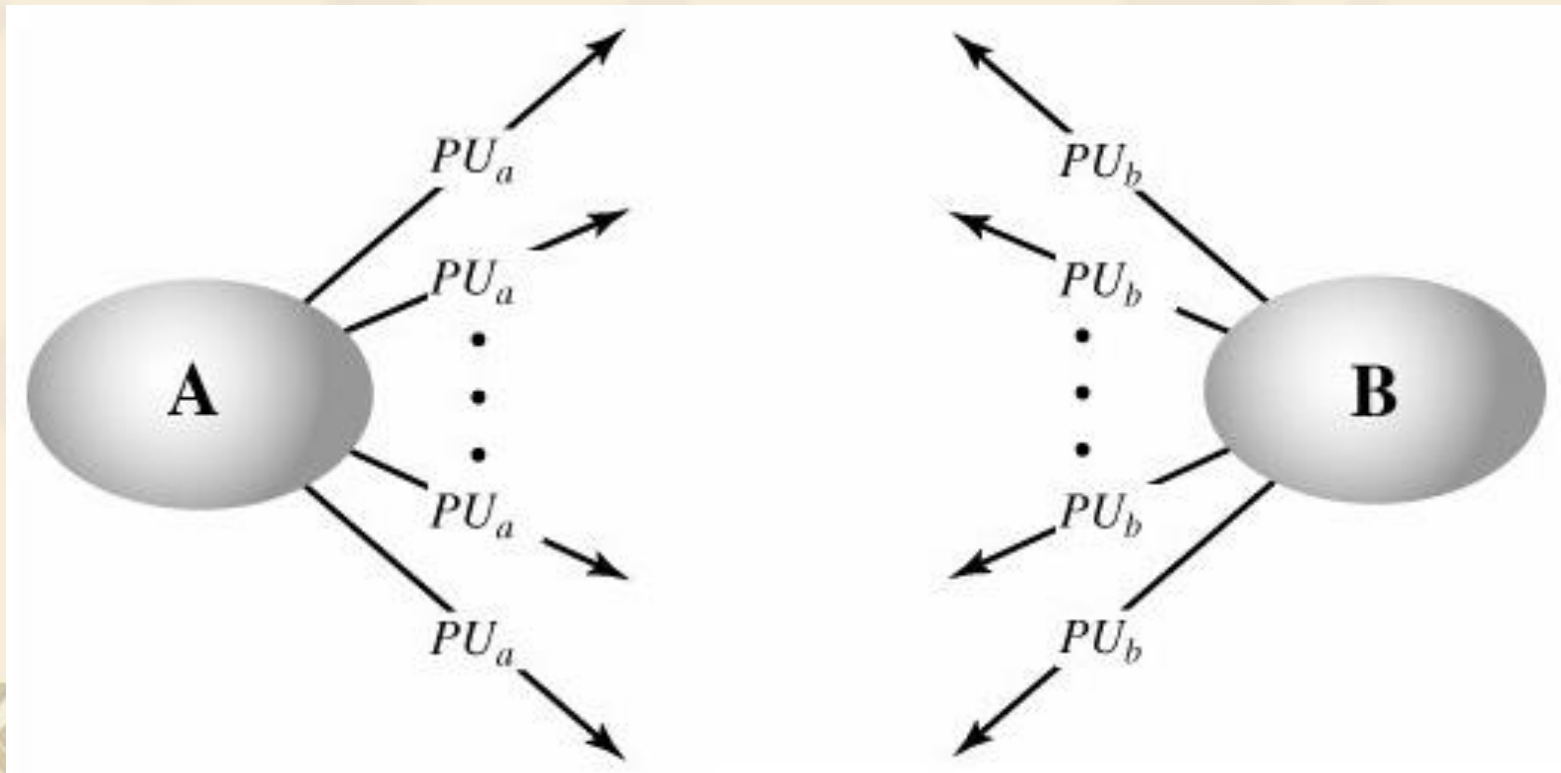
❧ Publicly available directory 公开可访问目录

❧ Public-key authority 公钥授权

❧ Public-key certificates 公钥证书

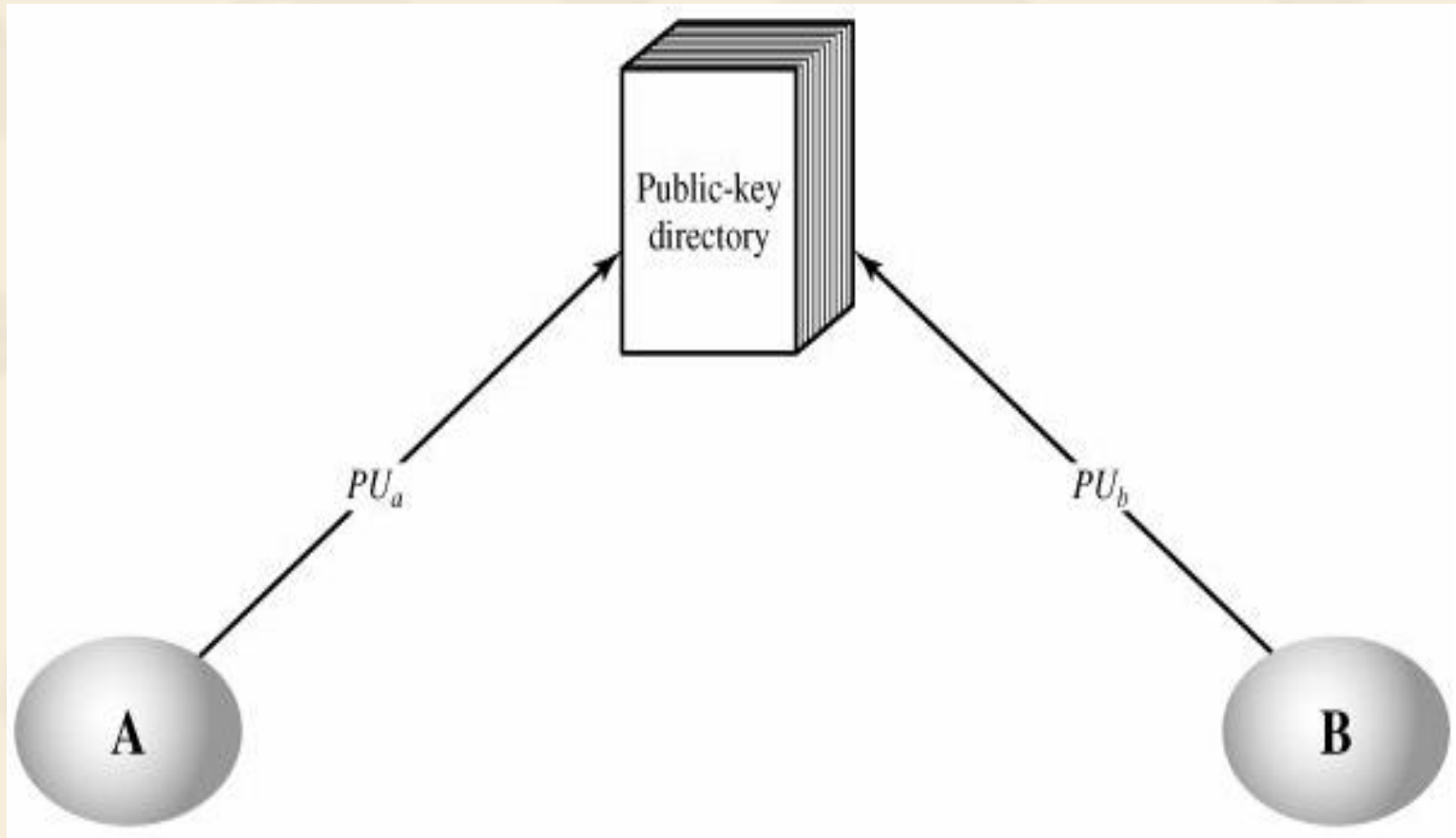
Public Announcement of Public Keys


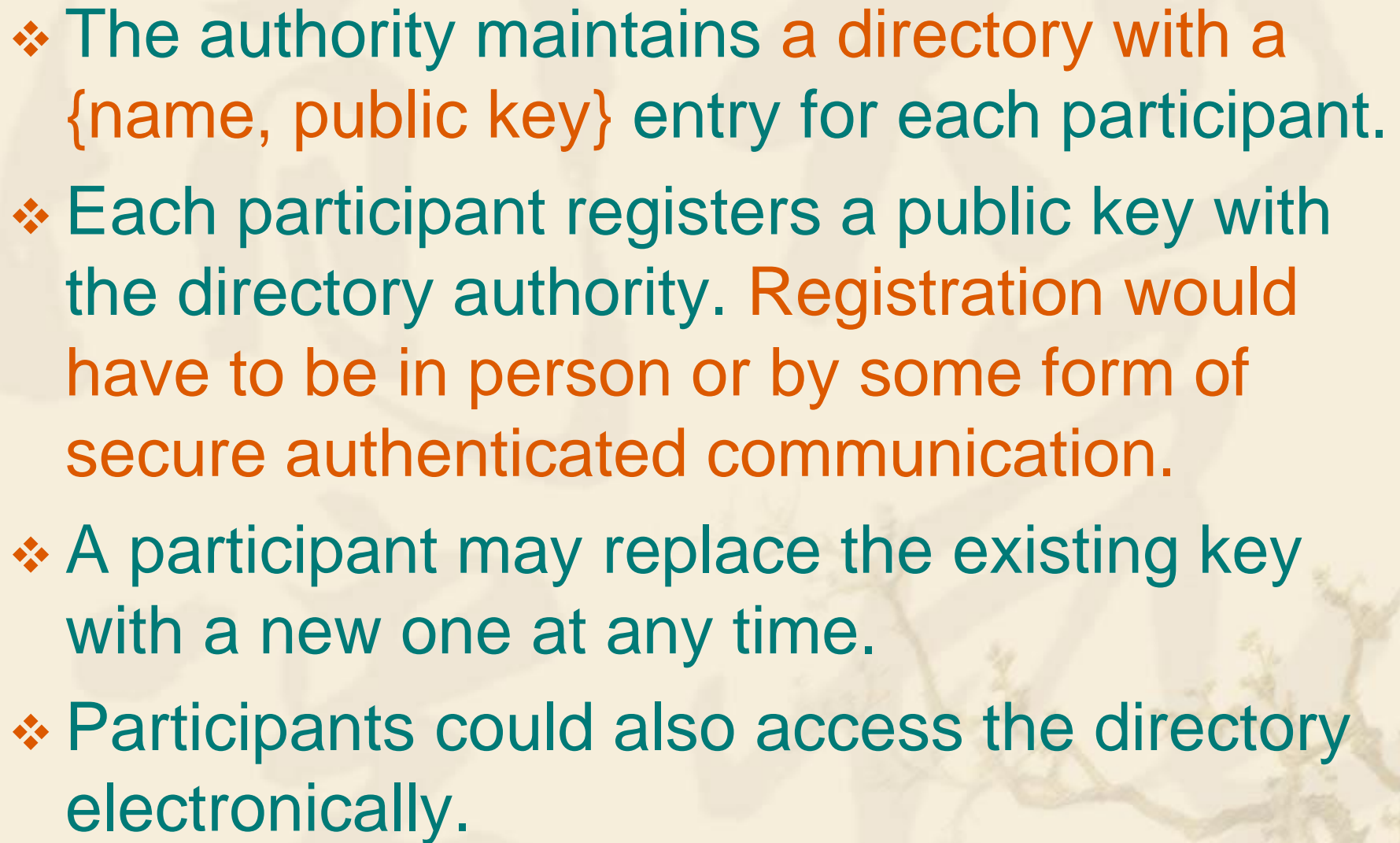
- ❖ Any participant can send his or her public key to any other participant or broadcast the key to the community, like BBS.



- ❖ Although this approach is **convenient**, it has **a major weakness**. Anyone can forge such a public announcement.
- ❖ Some user could pretend to be user A and send a public key to another participant or broadcast such a public key.
- ❖ Until such time as user A discovers the forgery and alerts other participants, **the forger is able to read all encrypted messages** intended for A and can use the forged keys for authentication.

Publicly Available Directory 公开可访问目录



- 
- 
- ❖ The authority maintains a directory with a {name, public key} entry for each participant.
 - ❖ Each participant registers a public key with the directory authority. Registration would have to be in person or by some form of secure authenticated communication.
 - ❖ A participant may replace the existing key with a new one at any time.
 - ❖ Participants could also access the directory electronically.

Public-Key Authority 公钥授权

- ❖ 公钥管理机构为用户建立维护动态的公钥目录。
- ❖ 每个用户知道管理机构的公钥。
- ❖ 只有管理机构知道自己的私钥。

公钥管理机构分配公钥



有可能成为系统的瓶颈，目录容易受到敌手的串扰

1.Request||Time1

- ❖ A发送一条带有时间戳的消息给公钥管理员，以请求B的当前公钥。

$$\underline{2.} \quad E_{SK_{AU}} [PK_B \parallel Request \parallel Time_1]$$

- ❖ 管理员给A发送一条用其私钥 SK_{AU} 加密的消息。这样如果A可以用管理员的公钥对接收到的消息解密，则可确信该消息来自管理员。
- ❖ 消息中的内容：
 - ∞ B的公钥 PK_B 。A可用它对要发送给B的消息加密。
 - ∞ 原始请求Request。A可用它与其最初发出的请求相比较，以验证其原始请求未被修改。
 - ∞ 原始时间戳Time1。A可以确定它收到的不是来自管理员的旧消息。

3. $E_{PK_B}[ID_A \parallel N_1]$

- ❖ A保存B的公钥，并用它对包含A的标识 ID_A 和临时交互号的消息加密，然后发给B。
- ❖ 临时交互号用来唯一标识本次交易。

4, 5


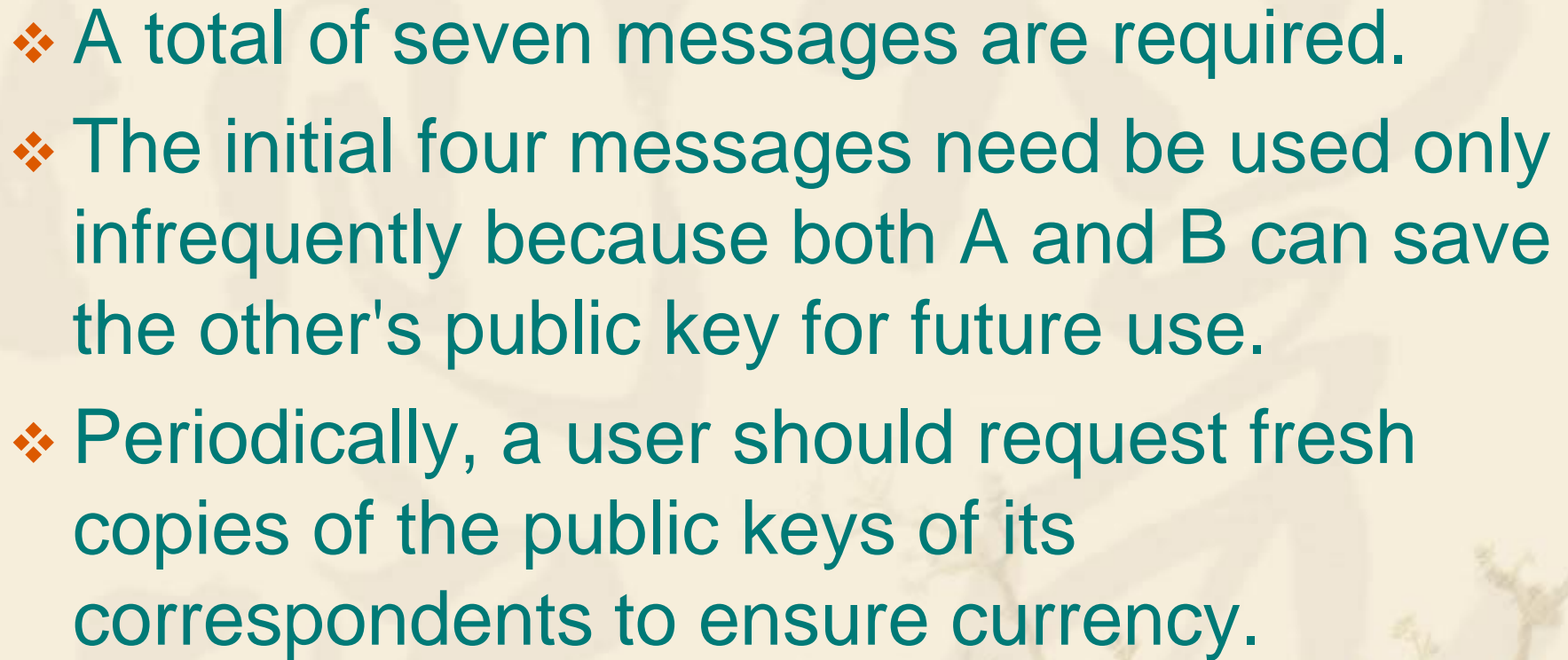
- ❖ B以同样的方法从管理员处得到A的公钥。

6. $E_{PK_A}[N_1 \parallel N_2]$

- ❖ B用 PK_B 对A的临时交互号N1和B产生的新临时交互号N2加密，并发送给A。因为只有B可以解密消息3，所以消息6中的N1可以使A确信其通信伙伴就是B。

7

- ❖ A用B的公钥对N2加密并发送给B，以使B相信其通信伙伴就是A。

- 
- 
- ❖ A total of seven messages are required.
 - ❖ The initial four messages need be used only infrequently because both A and B can save the other's public key for future use.
 - ❖ Periodically, a user should request fresh copies of the public keys of its correspondents to ensure currency.

Public-Key Certificates 公钥证书

- ❖ 在公钥授权方式下，用户要与其它用户通信，就必须向目录管理员申请对方的公钥，因此公钥管理员就会成为系统的瓶颈。
- ❖ Kohnfelder提出了使用证书的方法。
- ❖ 用户通过公钥证书交换各自公钥，无须与公钥管理机构联系

证书

主体身份信息

主体的公钥

CA名称

其他信息

CA签名

驾驶证

驾驶员身份信息

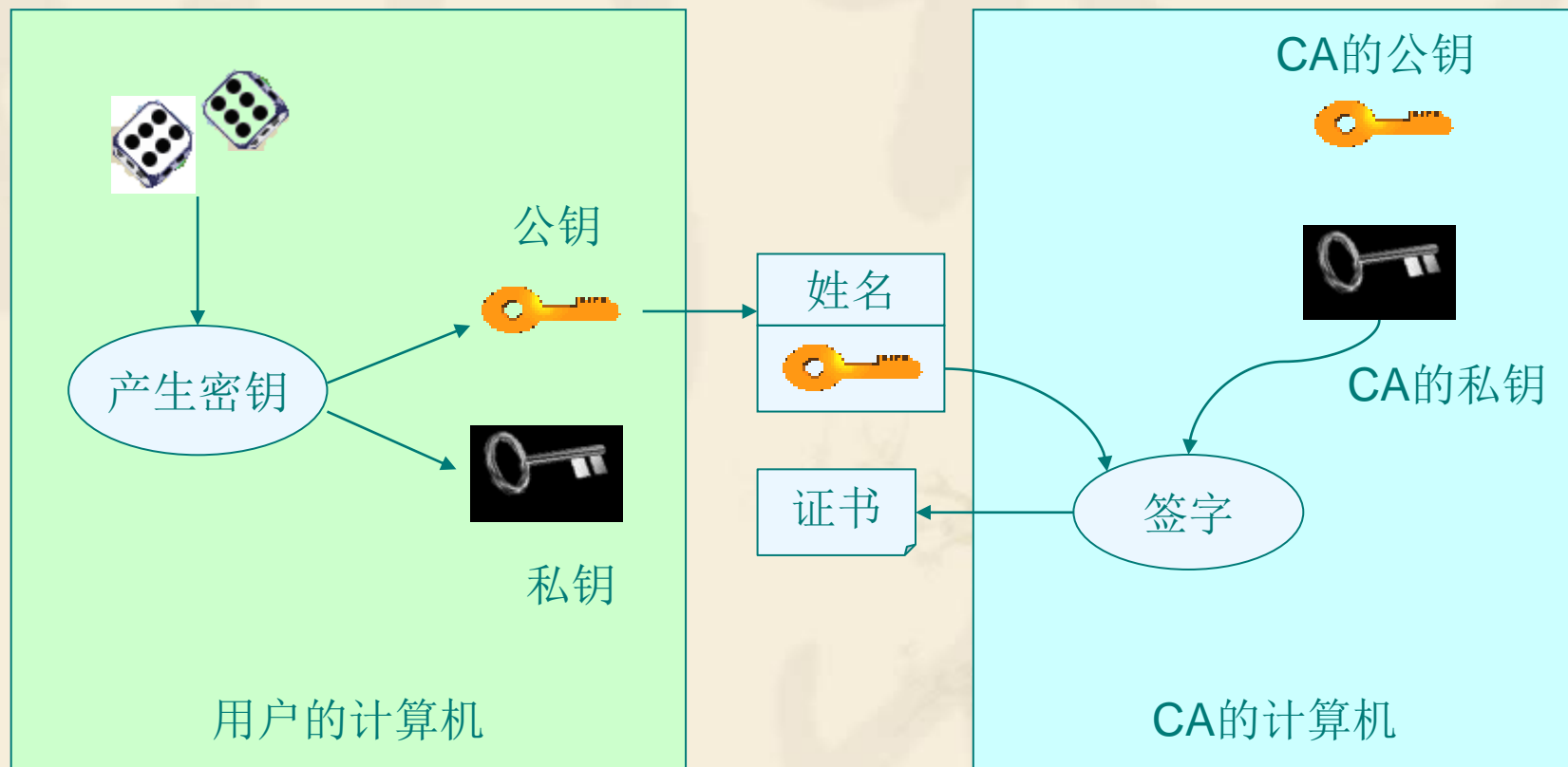
执照种类（驾驶能力）

公安局名称

其他信息

公安局盖章

证书的产生过程



公钥证书

- ❖ 用户通过公钥证书交换各自公钥，无须与公钥管理机构联系
- ❖ 公钥证书由证书管理机构 CA（Certificate Authority）为用户建立。
- ❖ 证书的形式为 $C_A = E_{SK_{CA}}[T, ID_A, PK_A]$
 - ∞ T-时间， PK_A -A的公钥， ID_A -A的身份， SK_{CA} -CA的私钥
- ❖ 时戳T保证证书的新鲜性，防止重放旧证书。

公钥证书方法须满足的条件

- ❖ Any participant can read a certificate to determine the name and public key of the certificate's owner.
- ❖ Any participant can verify that the certificate originated from the certificate authority and is not counterfeit.
- ❖ Only the certificate authority can create and update certificates.
- ❖ Any participant can verify the currency of the certificate.

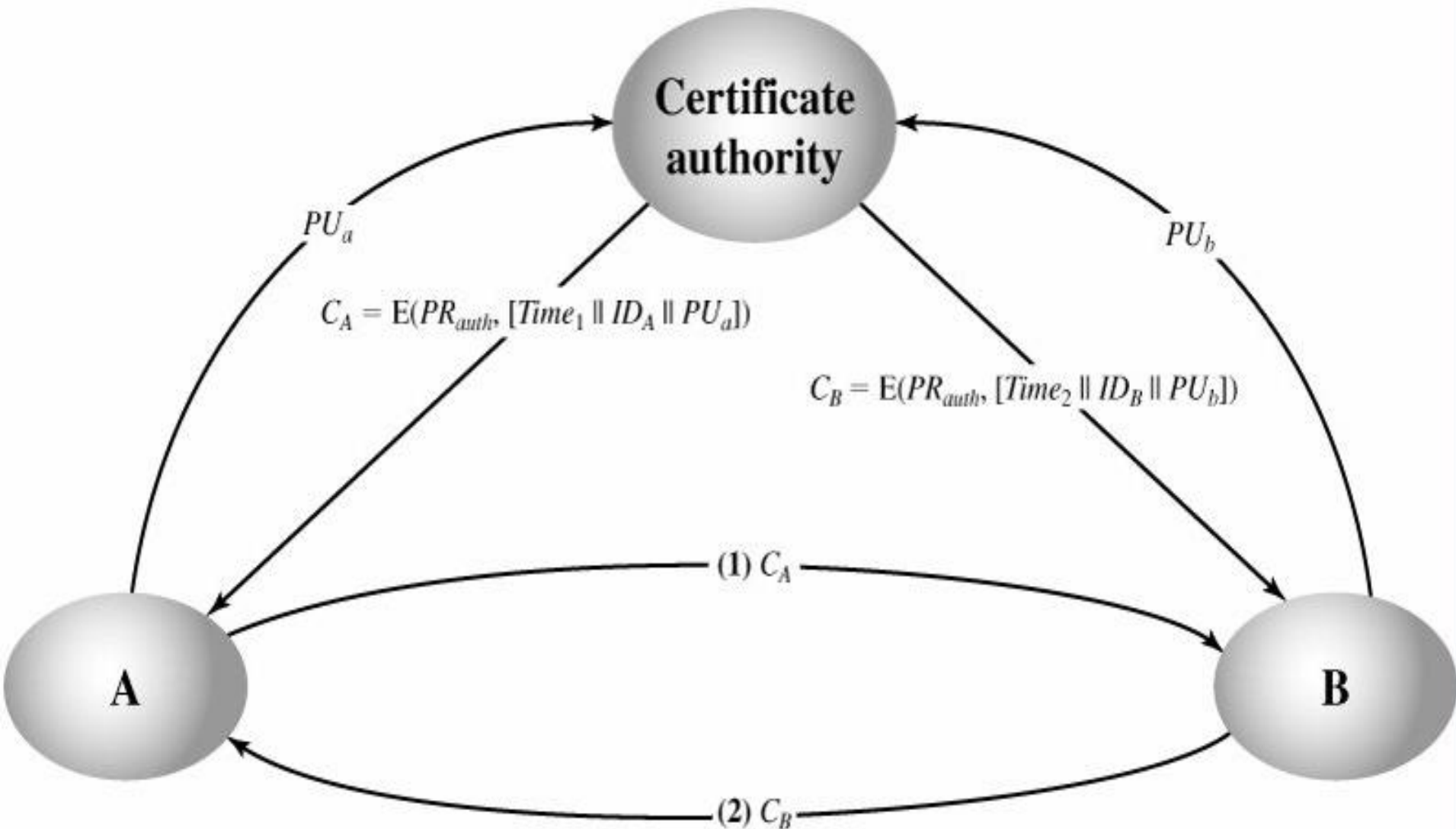
CA也为自己颁发公钥证书

- ❖ 由于公钥证书不需要保密，可以在Internet上分发，从而实现公钥的安全分配。有了签名，攻击者就无法伪造合法的公钥证书。因此，只要CA是可信的，公钥证书也是可信的。其中CA公钥的获取也是通过证书方式进行的，为此CA也为自己颁发公钥证书。
- ❖ 根证书---自签名证书

使用公钥证书的好处

- ❖ 用户只要获得其它用户的证书，就可以获得其它用户的公钥。
- ❖ 用户只要获得CA的公钥，就可以安全地认证其它用户的证书。
- ❖ 因此公钥证书为公钥的分发奠定了基础，成为公钥密码在大型网络系统中应用的关键技术。
- ❖ 这就是电子政务、电子商务等大型网络应用系统都采用公钥证书技术的原因。

Exchange of Public-Key Certificates

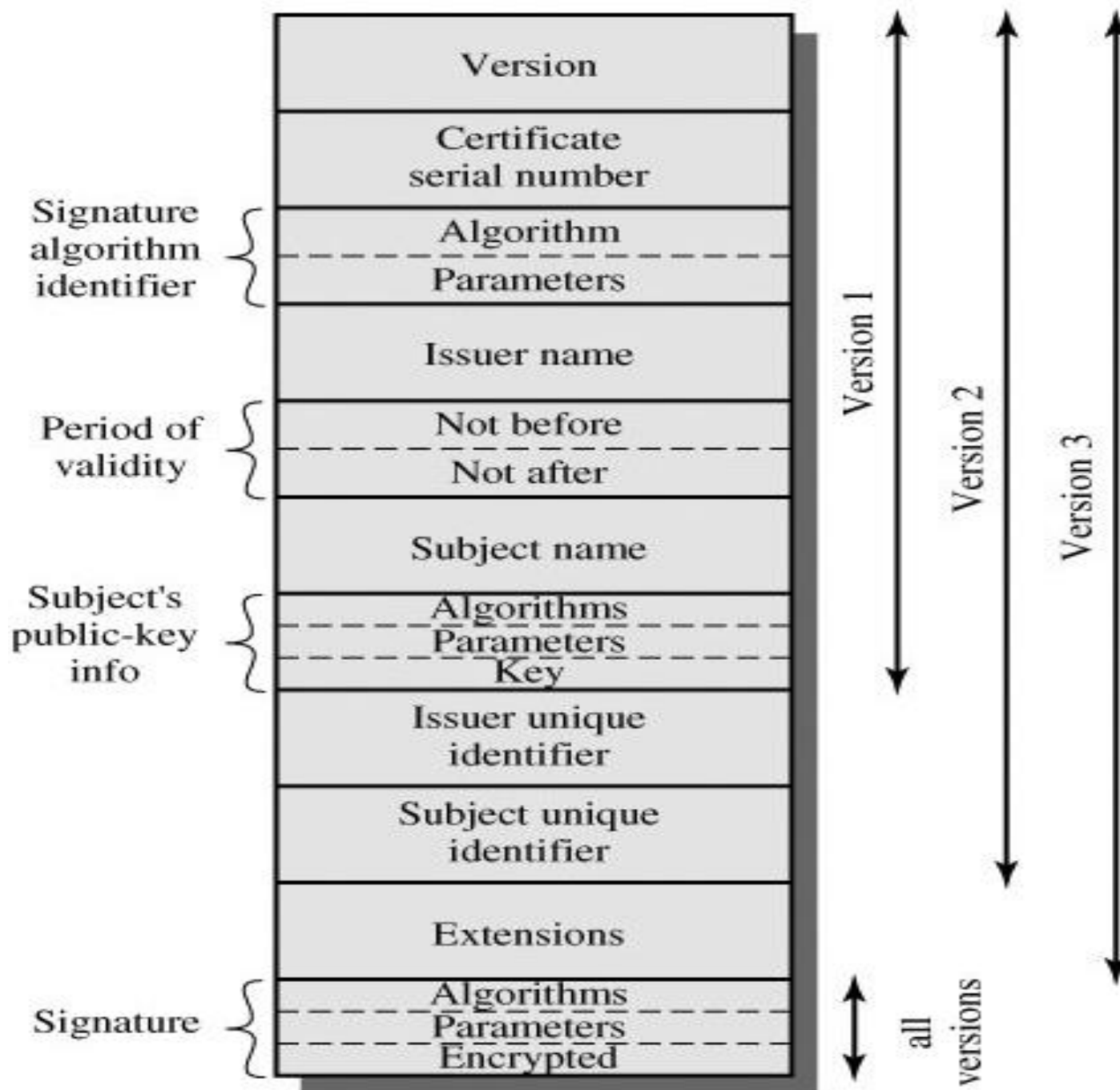


如何使用证书

- ❖ “客户” ->“服务器”：你好
- ❖ “服务器” ->“客户”：你好，我是服务器，这里是我的数字证书
- ❖ “客户” ->“服务器”：向我证明你就是服务器，这是一个随机字符串
- ❖ “服务器” ->“客户”：这是对随机字符串的签名
- ❖ 验证“服务器”的身份后，“客户”生成一个对称加密算法和密钥，用于后面的通信的加密和解密。这个对称加密算法和密钥，“客户”会用公钥加密后发送给“服务器”，别人截获了也没用，因为只有“服务器”手中有可以解密的私钥。这样，后面“服务器”和“客户”就都可以用对称加密算法来加密和解密通信内容了。

7.2.3 X.509证书

- ❖ 现实中有各种各样的证书，如PGP、SET、IPSec
- ❖ 目前应用最广泛的证书格式是国际电信联盟ITU提出的X.509版本3。
- ❖ X.509最早于1988年颁布，1993年和1995年两次修改。
- ❖ Internet工程任务组针对X.509在Internet环境的应用，颁布了一个作为X.509自己的RFC2459。



(a) X.509 certificate

X.509的格式

- ❖ 证书格式版本：版本1、版本2或者版本3
- ❖ 证书序列号：本证书的唯一标识
- ❖ 签名算法标识符：本证书使用的数字签名算法
- ❖ 发证者的名称：证书颁发者的可识别名
- ❖ 有效期：证书有效的时间段
- ❖ 主体名称：证书拥有者的可识别名（非空）
- ❖ 主体公钥信息：主体的公钥以及使用的公开密钥算法。
- ❖ 发证者唯一标识符：可选字段，很少使用
- ❖ 主体唯一标识符：可选字段，很少使用
- ❖ 扩展项：密钥和主体的附加属性说明
- ❖ 颁发者签名

公钥基础设施PKI

- ❖ 公钥基础设施---Public Key Infrastructure
- ❖ 基础设施---电力基础设施、交通基础设施。

公钥基础设施PKI

- ❖ 公钥证书、证书管理机构、证书管理系统、围绕证书服务的各种软硬件设备以及相应的法律基础共同组成公开密钥基础设施**PKI**。
- ❖ **PKI**是一种标准的密钥管理平台，它能够为所有网络应用透明地提供采用加密和数据签名等密码服务所必须的密钥和证书管理。
- ❖ 美国是最早(1996)推动**PKI**建设的国家。
- ❖ 1998年中国的电信行业建立了我国第一个行业**CA**，此后金融、工商、外贸、海关和一些省市也建立了自己的行业**CA**或地方**CA**。

公钥基础设施PKI

密码基础

基本理论



应用安全

经典的安全解决方案
PKI、数字证书、身份认证

网络攻防安全

公钥基础设施PKI

密钥对的用途

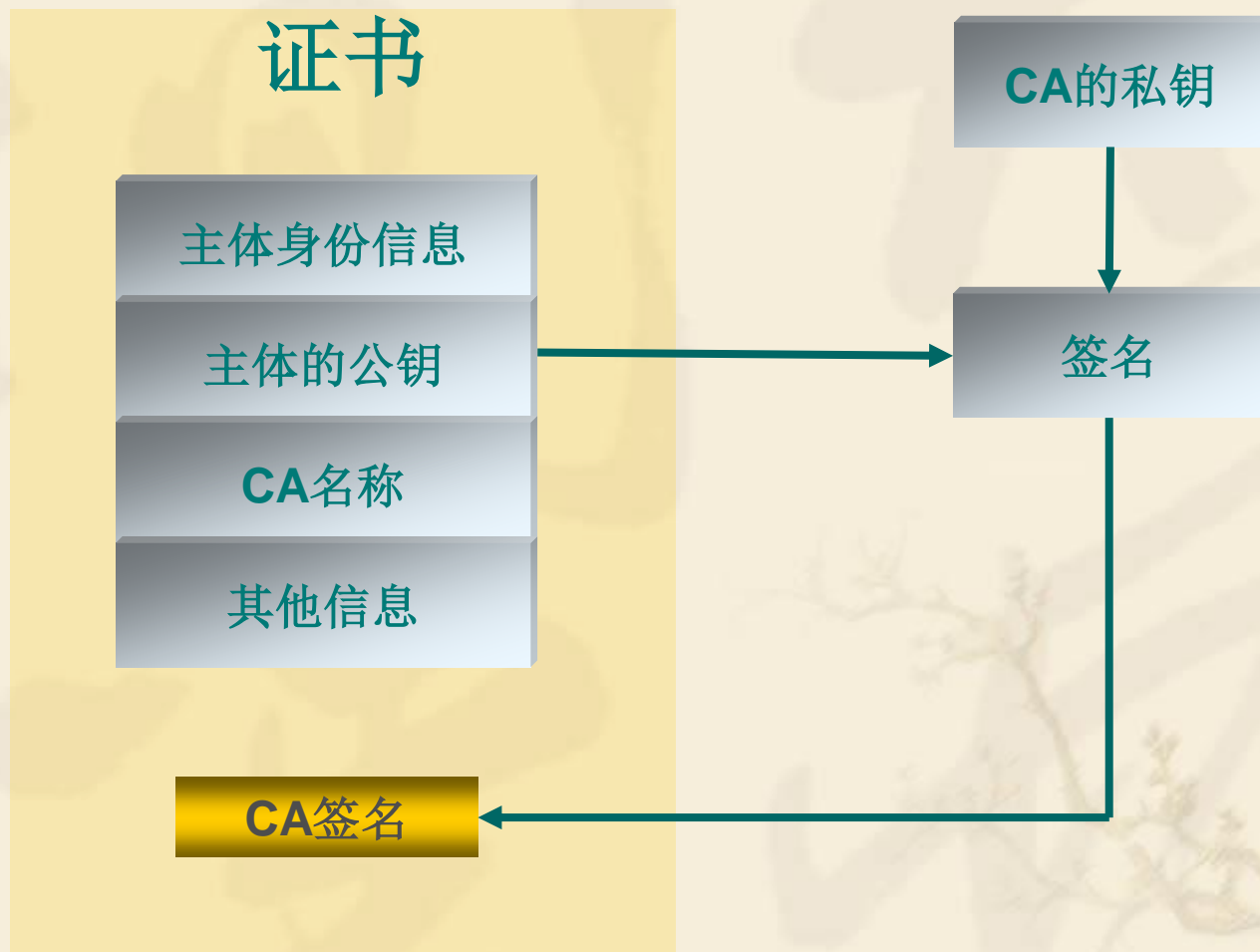
- ❖ 用于加密的密钥对---有效期---1-5年
公钥---加密
私钥---解密
- ❖ 用于签名的密钥对---有效期---1-3年
私钥---签名
公钥---验证

公钥基础设施PKI

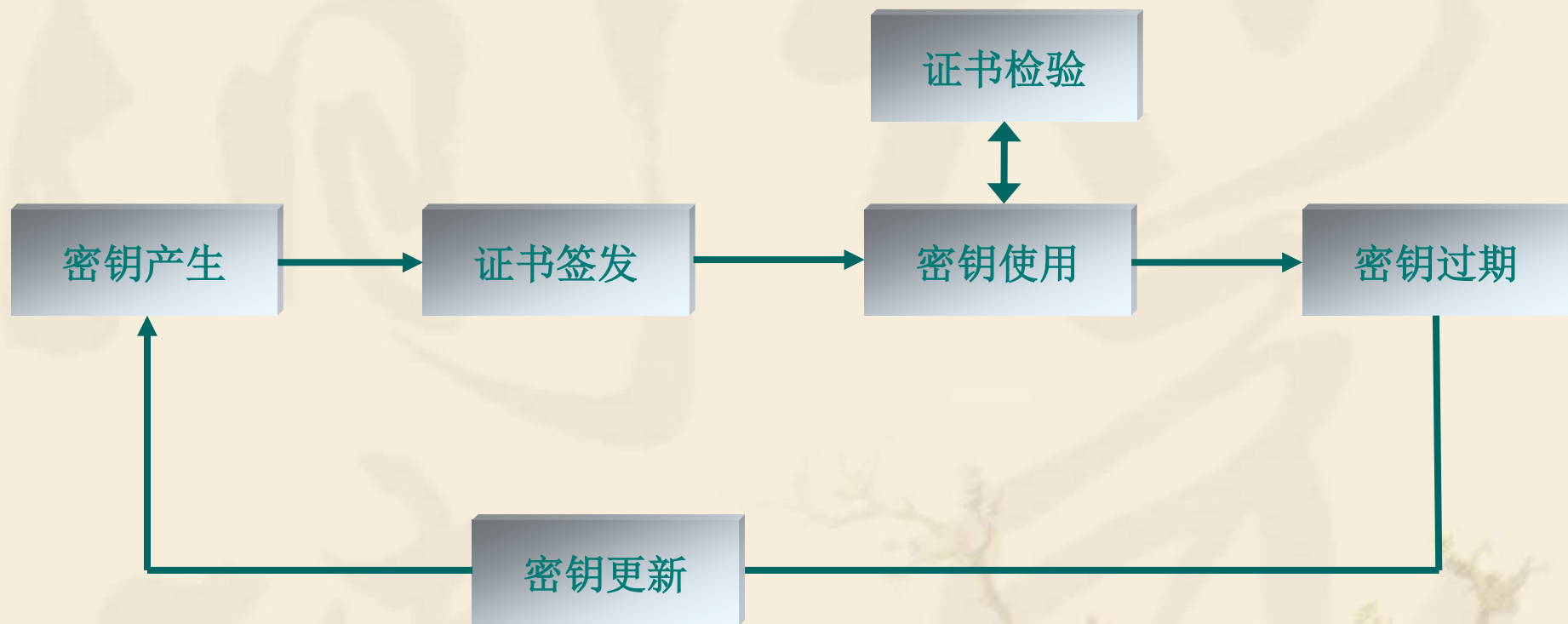
PKI解决的问题---实现公钥与身份的绑定

- ❖ 如何相信这是某个人的公钥？
 - ❖ 数字证书---Digital Certification
 - ❖ 证书授权中心---Certificate Authority
- 证书需要保密吗？完整性和可认证性。

公钥基础设施PKI



公钥基础设施PKI



密钥生命周期

公钥基础设施PKI

PKI：用公钥原理和技术实施和提供安全服务的普适性的安全基础设施。一个完整的**PKI**应该包括：

证书授权中心**CA**

证书库

证书注销

密钥备份和恢复

自动密钥更新

密钥历史档案

交叉认证----多**CA**、信任关系

支持不可否认

时间戳

客户端软件---支持证书查询、下载等

公钥基础设施PKI

数字证书

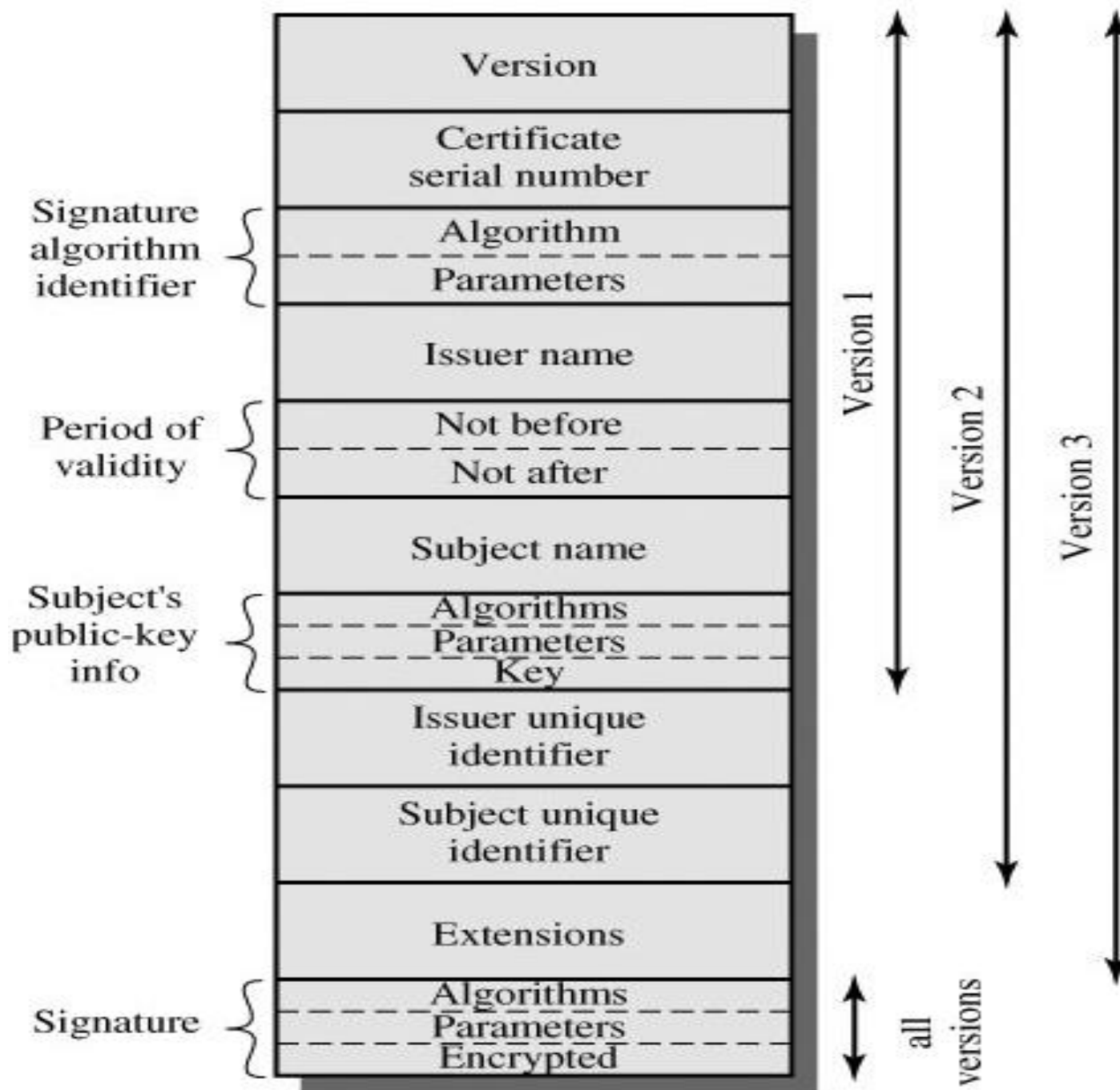
1.PKI中的证书-----Certificate,cert

- ❖ 证书是一个机构颁发给一个安全主体的证明，所以证书的权威性取决于该机构的权威性。
- ❖ 一个证书中重要信息：主体名字、主体的公钥、机构签名、算法和用途。
签名证书和加密正式分开。
- ❖ **PKI**适用于异构环境中，所以证书的格式在所使用的范围内必须统一。
- ❖ 常用的证书格式 **X.509v3**---遵循**X.509** 国际标准：实际是**X.500**的系列标准之一，证书内容还应表明证书的有效性。

公钥基础设施PKI

证书内容还应表明证书的有效性

- 1.证书没有过期，密钥没有修改，用户仍然有权使用这个密钥，**CA**负责收回证书，发行无效证书清单。
- 2.证书使用：证书帮助证实个人身份，你的证书和密钥就是你是谁的证据。

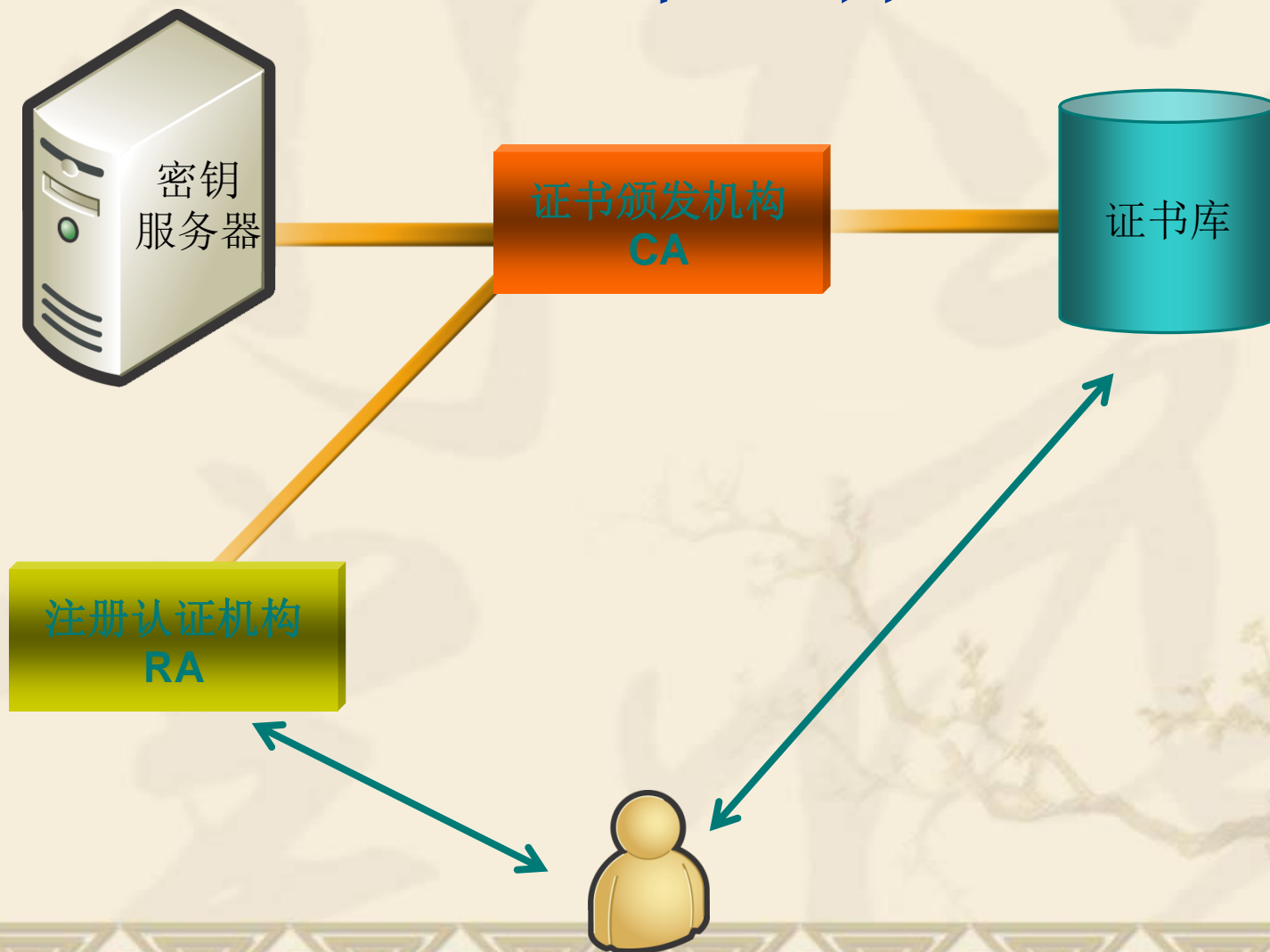


(a) X.509 certificate

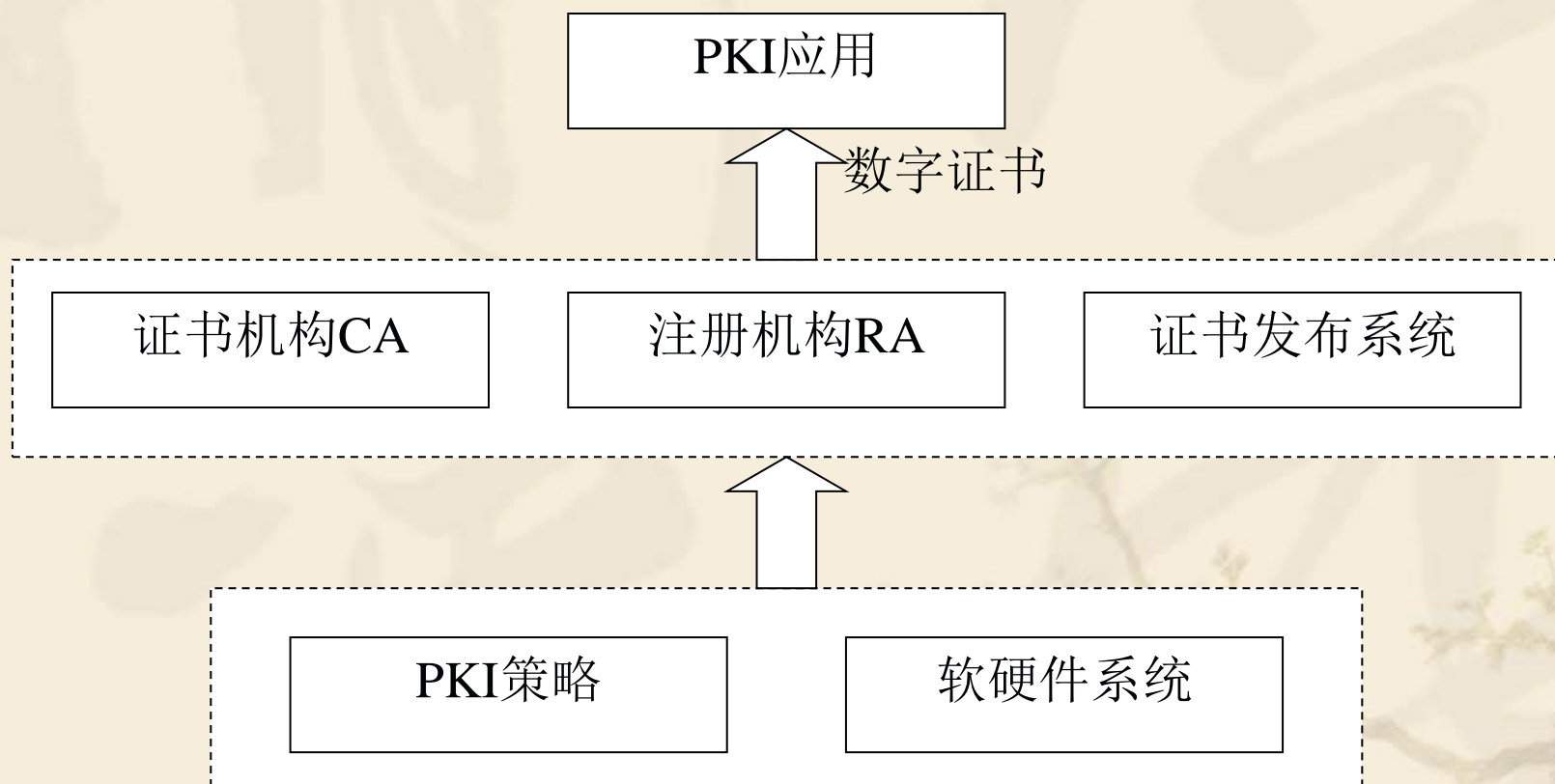
公钥基础设施PKI

PKI的主要目的是通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而保证网上数据的机密性、完整性和有效性。

PKI基本组件



PKI的逻辑结构



公钥基础设施PKI

PKI组成

- ❖ 软硬件系统：支持整个**PKI**信息系统运行的各种基础软硬件环境，如操作系统、网络环境等。
- ❖ **PKI策略**：**PKI**安全策略建立和定义了一个组织信息安全方法的指导方针，同时，也定义了密码系统使用的处理方法和原则，它包括一个组织怎么样处理密钥和有价值的信息，根据风险级别定义安全控制的级别。

公钥基础设施PKI

PKI组成

- ❖ 证书机构**CA**：是**PKI**的信任基础，它管理公钥的整个生命周期，其作用包括发放证书、规定证书的有效期和通过发布证书撤销列表，确保必要时可以废除证书。
- ❖ 注册机构**RA**：提供用户和**CA**之间的一个接口，获取并认证用户的身份，向**CA**提出证书请求。它主要完成收集用户信息和确认用户身份的功能。这里的用户，是指将要向认证中心**CA**申请数字证书的客户，可以是个人，也可以是集团或团体、政府机构等。

公钥基础设施PKI

PKI组成

- ❖ 证书发布系统：负责证书的发放，如可以通过用户自己，或是通过目录服务。目录服务器可以是一个组织中现存的，也可以是**PKI**方案中提供的。
- ❖ 数字证书：在**PKI**中，最重要的信息是数字证书，可以说，**PKI** 的所有活动都是围绕数字证书进行的。
- ❖ **PKI** 应用：其应用范围很广泛，并且在不断发展中，可以说只要需要使用公钥的地方就要使用到**PKI**，如安全电子邮件、**Web**安全、**VPN**等。

注册机构RA

- ❖ 专门负责受理用户申请证书
- ❖ 对证书申请人的合法性进行认证，并决定是批准或拒绝证书申请，不负责签发证书。
- ❖ 接收和授权密钥备份和恢复请求；
- ❖ 接收和授权证书吊销请求；

注册认证机构
RA

证书颁发机构CA

- ❖ 公钥证书的颁发机构,也负责证书的管理和撤销。
- ❖ 证书包含了用户的公开密钥, 权威性文档
- ❖ CA是所有注册用户所信赖的权威机构。
- ❖ CA用自己的私钥对证书签名。
- ❖ CA也给自己颁发证书。
- ❖ 对于大范围的应用, 一个CA是不够的。一个CA和少量的用户不能成为PKI。

证书颁发机构
CA

- ❖ 对于一个小范围的系统，由CA兼管RA的职能也是可以的。
- ❖ 但随着用户的增多，CA与RA应当职责分开。
- ❖ 申请证书的方式：
 - ☞ 在线的：WEB浏览器方式
 - ☞ 离线的

证书的签发过程

- ❖ 用户向CA提交RA的注册批准信息及自己的身份等信息(或者由RA向CA提供)
- ❖ CA验证所提交信息的正确性和真实性
- ❖ CA为用户产生密钥(或由用户自己产生并提供密钥), 并进行备份
- ❖ CA生成证书, 并施加签名
- ❖ 将证书的一个副本交给用户, 并存档入库

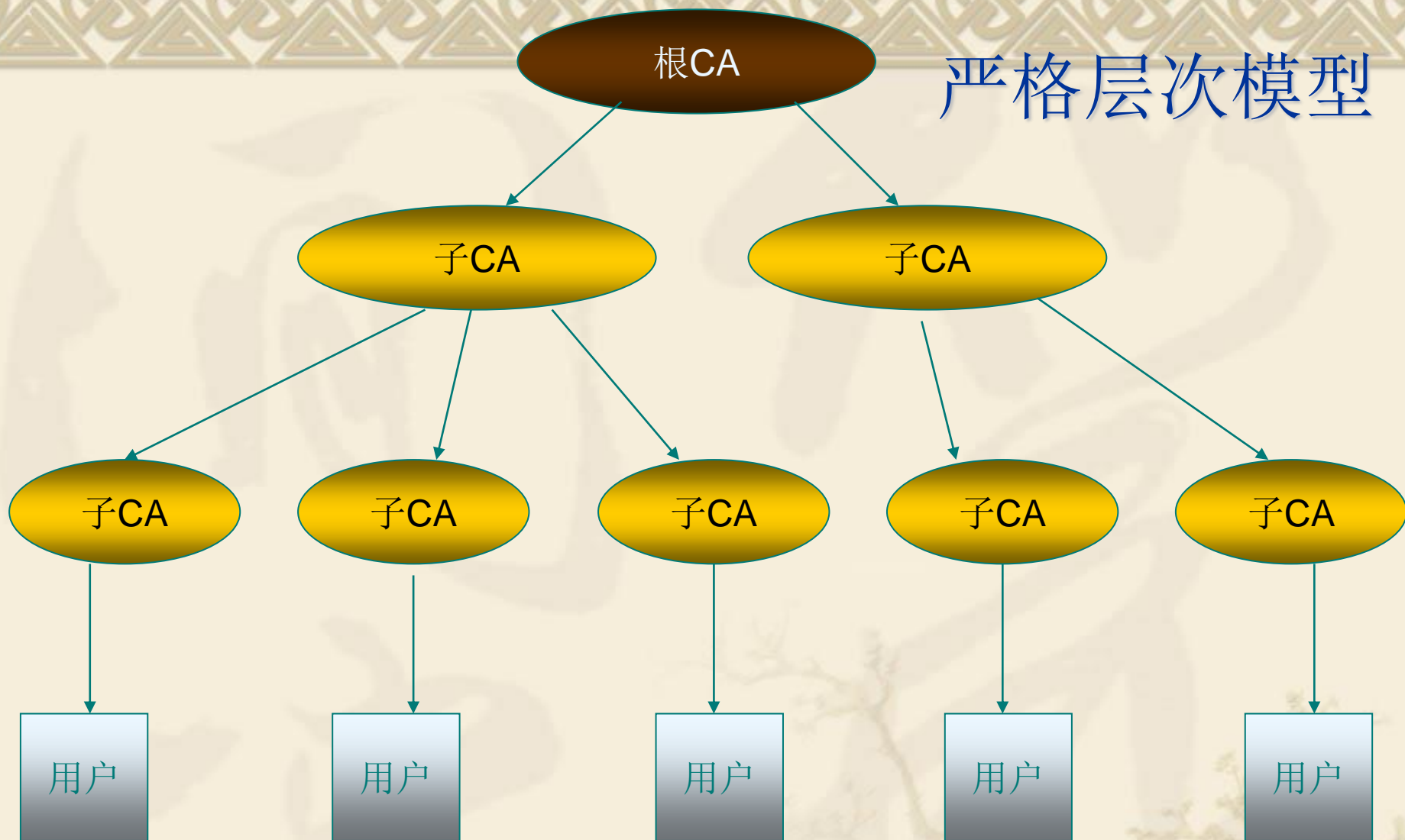
验证证书

- ❖ 验证证书上的**CA**签名是否正确。
- ❖ 验证证书内容的真实性和完整性。
- ❖ 验证证书是否处在有效期内（由证书里的时间参数来限定有效期）
- ❖ 验证证书是否被撤销或冻结。
- ❖ 验证证书的使用方式是否与证书策略和使用限制相一致。

PKI的信任模型

- ❖ 建立一个管理全世界所有用户的全球性**PKI**是不现实的。各个国家都建立自己的**PKI**，一个国家内部再分别建立不同行业或不同地区的**PKI**。
- ❖ 为了实现跨地区、跨行业，甚至跨国际的安全电子业务，这些不同的**PKI**之间的互联互通和相互信任是不可避免的。
- ❖ 对于大范围的**PKI**，一般会有很多的**CA**，这些**CA**之间应当具有某种结构的联系，以使不同**CA**之间的证书认证简单方便。
- ❖ 证书用户、证书主体、各个**CA**之间的证书认证关系称为**PKI**的信任模型。

严格层次模型



每个用户都有两个证书：子CA和根CA

Web模型

- ❖ 依赖于浏览器
- ❖ 将一些CA的公钥预装在使用的浏览器上
- ❖ 这些CA作为根CA

- ❖ 在操作系统刚安装好时(例如windows xp等操作系统)，一些证书发布机构的数字证书就已经被微软(或者其它操作系统的开发机构)安装在操作系统中了，微软等公司会根据一些权威安全机构的评估选取一些信誉很好并且通过一定的安全认证的证书发布机构，把这些证书发布机构的证书默认就安装在操作系统里面了，并且设置为操作系统信任的数字证书。

客服热线：12306



中国铁路客户服务中心

www.12306.cn是中国铁路客户服务中心唯一网站。截止目前，没有授



2015年11月22日 星期日

首页

客运服务

货运服务

行包服务

车站引导

铁路常识

站车风采

客户信箱



最新动态

为保障您顺畅购票，请下载安装[根证书](#)。

- 公告 (2015-10-31)
- 广铁集团公司关于2015年11月22日至11月25日海南东环线部分旅客列车... (2015-11-21)
- 广铁集团公司关于2016年2月7日至2月10日部分动车组列车临时停运的公告 (2015-11-21)
- 广铁集团公司关于2015年11月20日三亚开D7304次旅客列车临时停运的公告 (2015-11-19)
- 广铁集团公司关于2015年12月28日至2016年1月23日期间部分旅客列车临... (2015-11-19)
- 广铁集团公司关于2015年11月21日至11月26日期间Z201次等部分过海旅... (2015-11-19)
- 广铁集团公司关于2015年12月27日至2016年3月10日期间张家界—济南K1... (2015-11-19)

更多>>>

全文搜索: 请输入搜索条件

搜索



铁路客运

法律法规及规范性文件



铁路货运

法律法规及规范性文件

网上购票常见问题

铁路常识

货运办理常见问题



快捷舒适、省时省钱

我要
发货

中国铁路货运
电子商务平台

货物快运



主要营业站受理服务电话

高铁动卧、夕发朝至

旅客服务质量调查问卷

新版售票

点击进入>>



网上购票用户注册



购票



我的保险

一个例子

- ❖ 公司“ABC Company”花了1000块钱，向一个证书发布机构“SecureTrust CA”申请了一张证书
- ❖ 这个证书发布机构“SecureTrust CA”是一个大家公认并被一些权威机构接受的证书发布机构，我们的操作系统里面已经安装了“SecureTrust CA”的证书。
- ❖ “SecureTrust CA”在给我们发布证书时，把Issuer, Public key, Subject, Valid from, Valid to等信息以明文的形式写到证书里面，然后用一个hash算法计算出这些数字证书内容的一个摘要，并把摘要用自己的私钥进行加密，然后和证书的内容一起发布
- ❖ 同时“SecureTrust CA”还会给“ABC Company”公司相应的私钥。
- ❖ 投入使用...

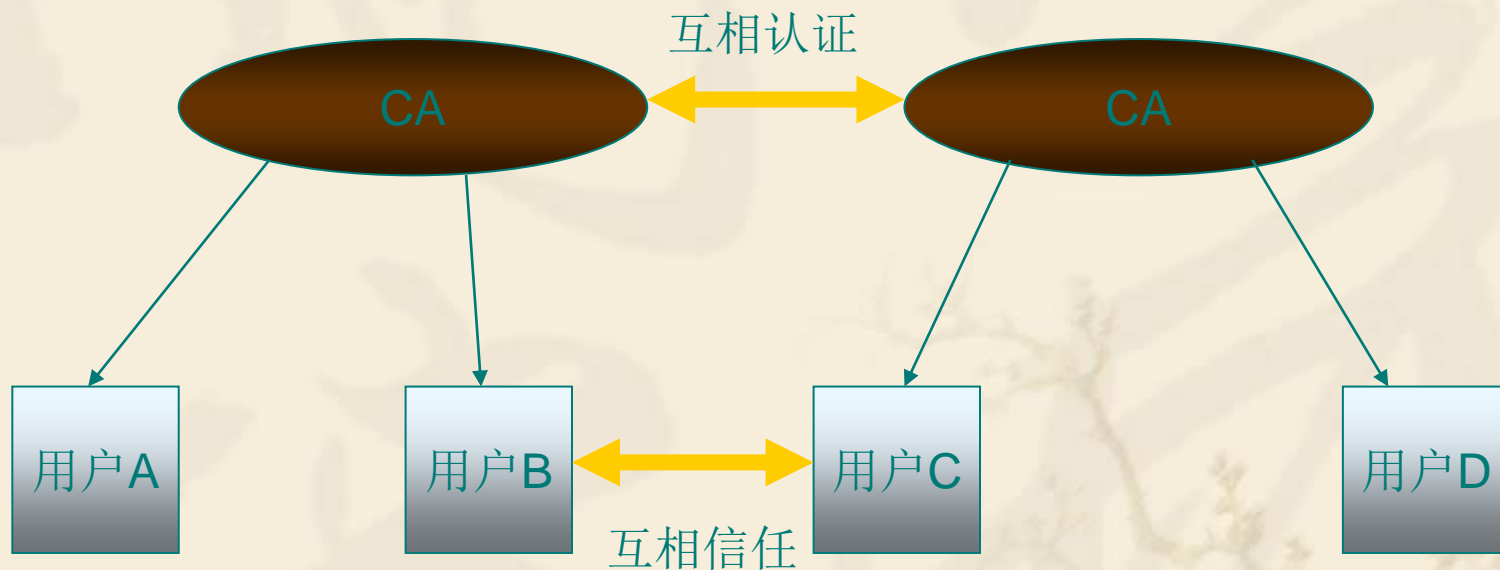
- ❖ 在通信过程开始时“ABC Company”会把证书发给对方，对方如何检查这个证书的确是合法的并且是“ABC Company”公司的证书呢？
- ❖ 首先应用程序(对方通信用的程序，例如IE、OUTLook等)读取证书中的Issuer(发布机构)为“SecureTrust CA”，然后会在操作系统中受信任的发布机构的证书中去找“SecureTrust CA”的证书，如果找不到，程序会给出一个错误信息。
- ❖ 如果在系统中找到了“SecureTrust CA”的证书，那么应用程序就会从证书中取出“SecureTrust CA”的公钥，然后对“ABC Company”公司的证书里面的签名用这个公钥进行解密，然后使用hash算法计算“ABC Company”证书的摘要，将这个计算的摘要与放在证书中的摘要对比，如果一致，说明“ABC Company”的证书肯定没有被修改过并且证书是“SecureTrust CA”发布的，证书中的公钥肯定是“ABC Company”的。对方然后就可以放心的使用这个公钥和“ABC Company”进行通信了。

交叉认证

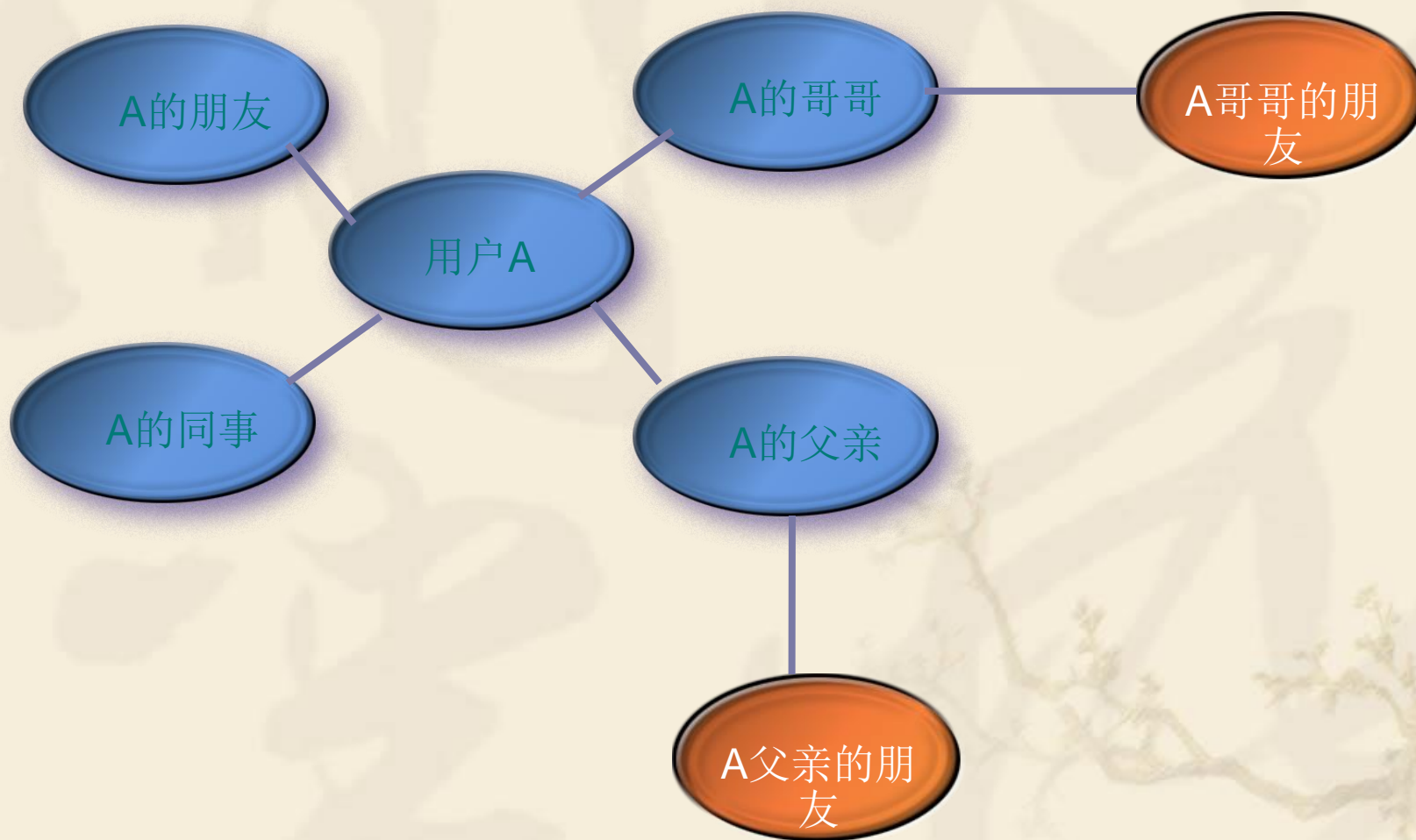
- ❖ CA之间互相发证书
- ❖ 用户控制的交叉认证

交叉认证模型

❖ 各个CA连接在一起



以用户为中心的信任



PKI应用

- ❖ Web安全问题范围以及使用PKI系统的对策
- ❖ 安全电子邮件实现原理与方案
- ❖ VPN实现原理与方案

Web安全

❖ 安全问题:

- ❧ 欺诈、泄露、篡改、攻击

❖ **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

- ❧ 认证用户和服务端

- ❧ 加密数据以隐藏被传送的数据

- ❧ 维护数据的完整性

安全电子邮件

- ❖ 在安全的电子邮件系统中，收发双方都有对方的数字证书。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。
- ❖ PGP
- ❖ S/MIME

VPN实现原理

- ❖ 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

PKI案例

- ❑ 电子税务
- ❑ 网上银行
- ❑ 网上证券



湖北省数字证书认证管理中心有限公司
HuBei Digital Certificate Authority Center Co.,Ltd

内部邮箱 员工专区 进入旧版

客服热线：400-676-7799

首页

公司简介

产品与方案

客户服务

法律法规

成功案例

渠道与合作

联系我们



公司简介

当前位置：首页 - 公司简介

- > 公司简介
- > 企业文化
- > 资质证明
- > 招贤纳士

公司简介

湖北省数字证书认证管理中心有限公司（以下简称“湖北CA”）成立于2000年4月，注册资金5000万元，是经湖北省政府批准成立、省内唯一获得国家工业和信息化部颁发的《电子认证服务许可证》和国家密码管理局颁发的《电子认证服务使用密码许可证》的合法电子认证服务机构，目前控股方为湖北省信息中心。

湖北CA是湖北省网络信任体系的重要组成部分，是湖北省电子政务门户CA认证的唯一授权服务商。公司致力于电子政务、电子商务领域电子认证业务，可提供方案设计、技术支撑及咨询培训等信息安全服务，保证电子政务及电子商务活动双方身份的真实性、通信信息的保密性、交换数据的完整性、交易行为的不可否认性以及访问权限的可控性。

湖北CA采用经国家密码管理局技术鉴定的数字证书认证系统，建有高度安全的CA中心、密钥管理中心等安全基础设施，技术先

服务直通车

- ◆ 电子认证业务规则
- ◆ 根证书下载/安装
- ◆ 证书实体查询
- ◆ 老用户CRL下载
- ◆ 新用户CRL下载
- ◆ 责任书下载

电子税务

❖ 安全需求

- ❧ 通信安全
- ❧ 身份认证与访问控制
- ❧ 业务安全

❖ 解决方案

- ❧ 通信安全：**SSL**
- ❧ 身份认证与访问控制：数字证书
- ❧ 业务安全：数字签名

网上银行

❖ 安全需求

- ❧ 身份认证
- ❧ 通信安全
- ❧ 访问控制
- ❧ 审计安全

❖ 实施方案

银行客户先申请数字证书，再使用数字证书通过SSL通道来登录网上银行的相关业务系统来进行网上交易。

网上证券

❖ 安全需求

- ❧ 通信安全

- ❧ 身份认证与访问控制

- ❧ 业务安全

❖ 实施方案

通过配置**PKI**来实现



第三方认证机构



最终用户

