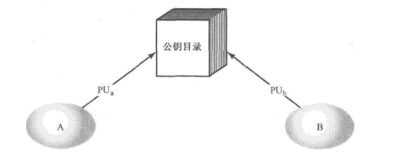
**解决什么问题？**

　　公钥分发是为了解决公钥伪造的问题。虽然每个用户的公钥是公开的，但是任何人都可以伪造其他用户的公钥并广播或者传给特定用户。

**解决方案**

**公开可访问的目录**

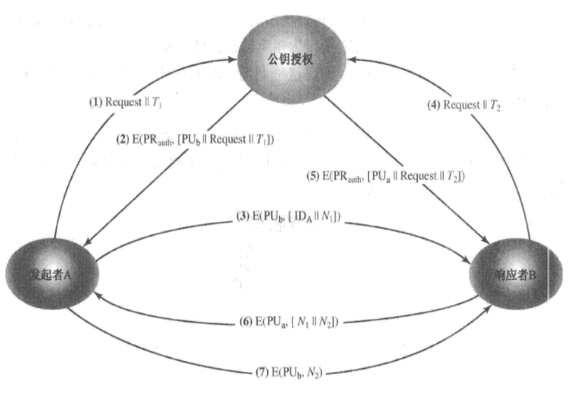
由可信实体维护和分配公开目录，目录项记录着每个通信方的身份和公钥。每个通信方必须通过安全的认证通信注册或更换自己的公钥以及访问其他用户的公钥。



　　　　缺陷：由于公钥目录完全公开，攻击者可以入侵目录管理者修改目录或者扮演目录管理者。

**公钥授权**

公钥授权是在公开目录基础上做了改进，管理员生成一对公私钥对，用私钥加密目录，再引进一系列验证来完成用户公钥的可靠传递，攻击者若没有私钥无法修改目录。

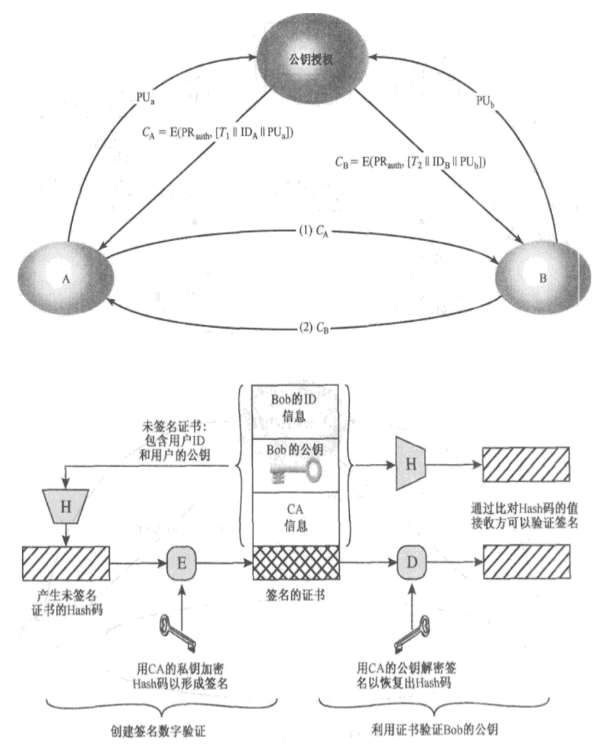


　　T是时间戳，N是临时交互号。

**公钥证书**

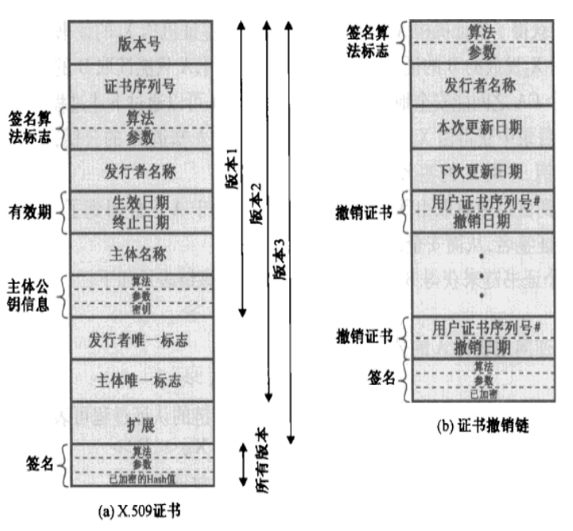
　　　　上面两种方法的都依赖于目录管理员，每次会话都需要访问目录管理员，因此目录管理员就会成为系统的瓶颈。

　　　　公钥证书进一步做了改进，通过引进第三方的数字签名生成公钥证书交由通信方自行管理，一次签证重复使用，解决了第三方通信瓶颈的问题。



　　目前广泛用于规范公钥证书的标准是X.509标准。

**X.509认证服务**



　　　　该标准采用如下标注定义证书：

　　　　　　CA《A》 = CA{V , SN , AI , CA , UCA , A , UA , Ap , TA}

　　　　　　　　Y《X》b表示用户X的证书是签证机构Y发放的

　　　　　　　　Y{I}表示Y签名I，包含I和I被加密后的Hash值

　　　　　　　　SN表示证书的序列号

　　　　　　　　AI表示用于给证书签名的算法的标志

　　　　　　　　CA表示签署证书机构的名称

　　　　　　　　UCA表示CA的可选择的唯一标志

　　　　　　　　A表示用户A的名称

　　　　　　　　UA表示A的可选择的唯一标志

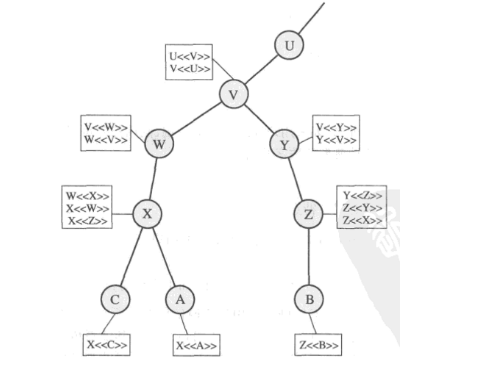
　　　　　　　　Ap表示用户A的公钥

　　　　　　　　TA表示证书的有效周期

　　　　　　CA用自己的私钥签署证书，如果用户知道相应的公钥就能验证证书是CA签署的。

　　　　如果A、B的公钥证书由不同的CA签证，则可通过不同CA之间的相互签证来获取彼此的公钥，推荐采用层次结构放置CA证书，以利于建立强大的导航功能。

　　　　　　每个CA目录入口中包含两种证书：前向证书和后向证书



　　　　这个图有点问题，每个节点应该是存自己签证的证书和自己被其他CA签证的证书

**公共基础设施PKI    　　　　Public Key Infrastruction**

　　PKI 系统是由硬件、软件、人、策略和程序构成的一整套体系，用以创建、管理、存储、分发和撤销建立在非对称密码算法之上的数字证书。

　　　　PXIX模型是在X.509标准基础上建立的认证体系的基本模型

