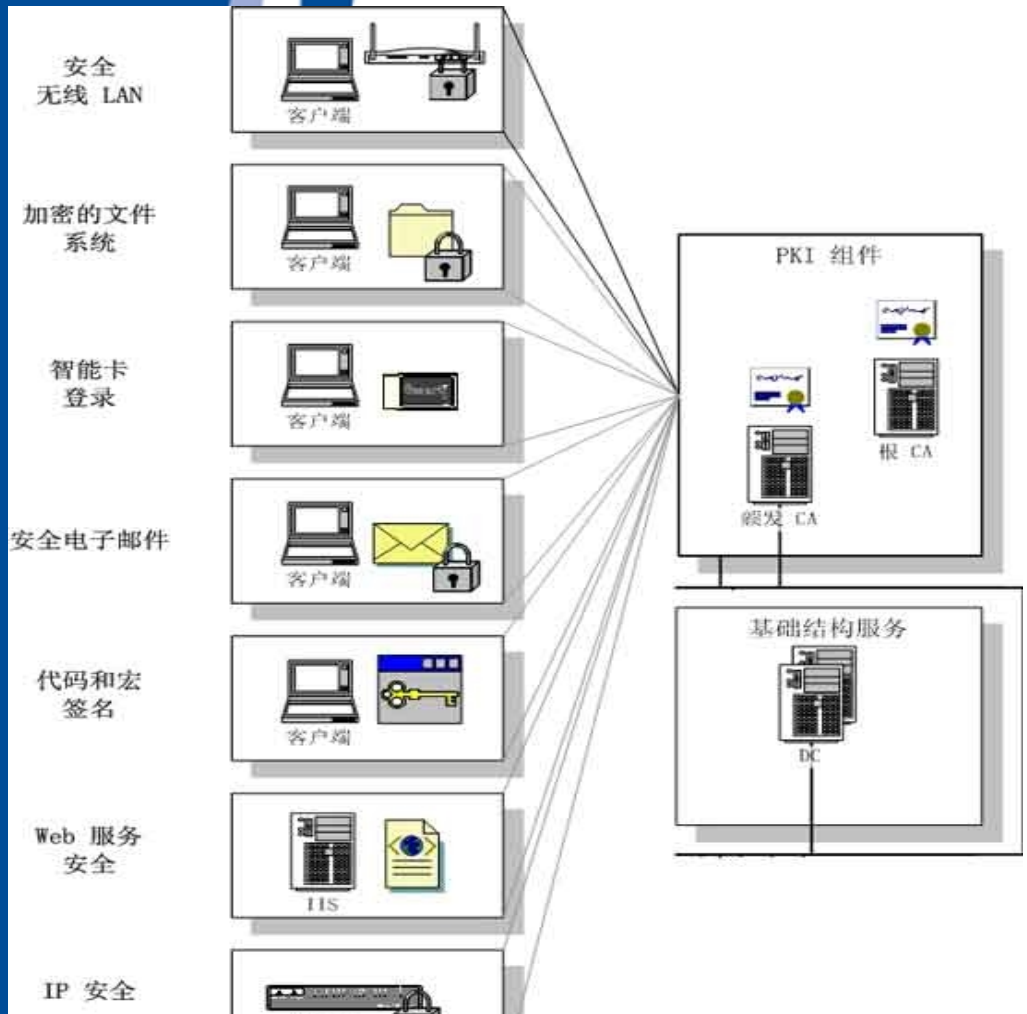
新华电脑教育
XINHUA COMPUTER EDUCATION
团结 务实 开拓 奉献

第10章　PKI



本章目标

- 1. PKI的基本概念
- 2. 数字证书的概念和使用
- 3. PKI的组成和功能
- 4.PKI的实际运用

10.1 PKI简介

10.1.1PKI的概念—为什么需要PKI?

互联网困境：

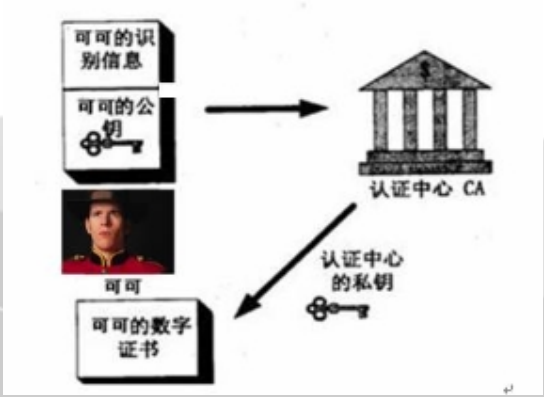
On the Internet, nobody know you're a dog.

公钥密码体制的局限

- 公钥密码体制的出现虽然解决了对称密钥的分配问题，但又产生了“公钥如何可信地在大范围内传播的问题”。
- 问题在于在Internet中很难统一管理“信任”，这一错综复杂的特性。
  - 例如：用户A如何确认用户B的公钥？会不会有人冒充用户B呢？

？什么是PKI

- PKI(公钥安全基础设施)是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，用来建立不同实体之间的“信任”关系。
- 他的基础技术包括：加密、数字签名、数字摘要、数字信封、双重数字签名等，核心是数字证书，并且具有可信任的权威机构CA，交易各参与方都信任这个CA，由CA来核对和验证各参与方的身份。



基础设施的概念

- 什么是基础设施：就是“只要遵循需要的原则，不同的实体就可以方便地使用基础设施提供的服务”
- 例如，电力基础设施：电源插座可以提供各种电力设备运行所需的电压和电流；当我们使用电器时只要把插头插上就可以了。
- 对于PKI来说同样是这个道理，不过与PKI相对应的应用是指需要安全服务而使用的的软件，例如：IE浏览器，OUTLOCK电子邮件程序等。

10.2 PKI组成

- 公钥证书
- 证书作废列表
- 策略管理机构
- 认证机构
- 注册机构
- 证书管理机构
- 证书存档
- 署名用户
- 依赖方
- 终端用户

PKI 系统的组成

- 1、证书申请者与证书信任者：

证书申请者是证书的持有者，证书的目的是把用户的身份与其密钥绑定在一起。

证书信任者是证书认证的另一方.在交易过程中可以提供证书也可以不提供证书.

2.注册机构

根据PKI的管理政策，RA的主要功能是核实证书申请者的身份，这项功能通常由人工完成，也可以由机器自动完成。注册机构本身并不发放数字证书,但注册机构可以确认,批准和拒绝证书申请人的申请,随后由认证机构给给经过批准的人发放证书。

- RA的功能如下：
  （1）验证申请者身份
  （2）批准生成证书的请求
  （3）批准证书更新和撤消的请求
  （4）将证书请求信息发送给CA

3、认证中心（CA）

PKI的管理机构，又称认证机构，证书授权中心，是承担网上认证服务，能签发数字签名并能够确认用户身份和受大家信任的第三方认证机构，其主要任务是受理证书的申请，签发，对数字证书的管理。 CA证书的签发机构可以看成是一个国家的护照签发中心。它是护照持有者的一种纸质身份证明，任何信任该国护照签发中心的其他国家也会信任该国护照签发中心所签发的护照。

- CA的功能如下：
  （1）批准由RA提交的证书请求
  （2）生成密钥对
  （3）密钥的备份
  （4）签发证书（发往证书库）
  （5）证书发放
  （6）撤销或更新证书
  （7）发布证书作废表（CRL）

4. 证书库

- 证书库存放了经CA签发的证书和已撤销证书的列表，网上交易的用户可以使用应用程序，从证书库中得到交易对象的证书、验证其证书的真伪、或查询其证书的状态。

- 证书库的功能如下：

（1）存储证书

（2）提供证书

（3）确认证书状态

5.密钥备份及恢复系统

- 如果用户丢失了用于解密数据的密钥，则数据将无法被解密，这将造成合法数据丢失。为避免这种情况，PKI提供备份与恢复密钥的机制. 用来对密钥的恢复