§6.3 公钥基础设施PKI

PKI（Public Key Infrastructure）

- 公钥密码的服务：
  - 陌生人之间的安全
  - 加密
  - 数字签名
  - 数据完整性
  - 密钥的建立
- **PKI是经过多年研究形成的一套完整的Internet安全解决方案。它用公钥技术和规范提供用于安全服务的具有普适性的基础设施。用户可利用PKI平台提供的服务进行安全通信。**

§6.3 公钥基础设施PKI

- **PKI系统的组成：**
  - 认证中心CA
  - 注册机构RA
  - 证书库CR
  - 证书申请者
  - 证书信任方

前三部分是PKI的核心，证书申请者和证书信任方则是利用PKI进行网上交易的参与者。

§6.3 公钥基础设施PKI

- **PKI的功能：**
  - 证书产生与发放；　　证书撤销；
  - 密钥备份及恢复；　　证书密钥对的自动更新；
  - 密钥历史档案；　　支持不可否认；
  - 时间戳；　　交叉认证；
  - 用户管理(如登录、增删等)；
  - 客户端服务：理解安全策略，恢复密钥，检验证书，请求时间戳等。
  - 其他功能：支持用于认证的智能卡。

此外PKI的特性融入各种应用（防火墙、浏览器、电子邮件、网络OS）也正在成为趋势。

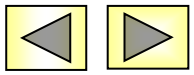
§6.3 公钥基础设施PKI



- 数字证书和PKI解决哪些问题：

数字证书能够解决信息传输的保密性、完整性、不可否认性、交易者身份的确定性问题。数字证书和PKI结合解决电子商务中的安全问题。

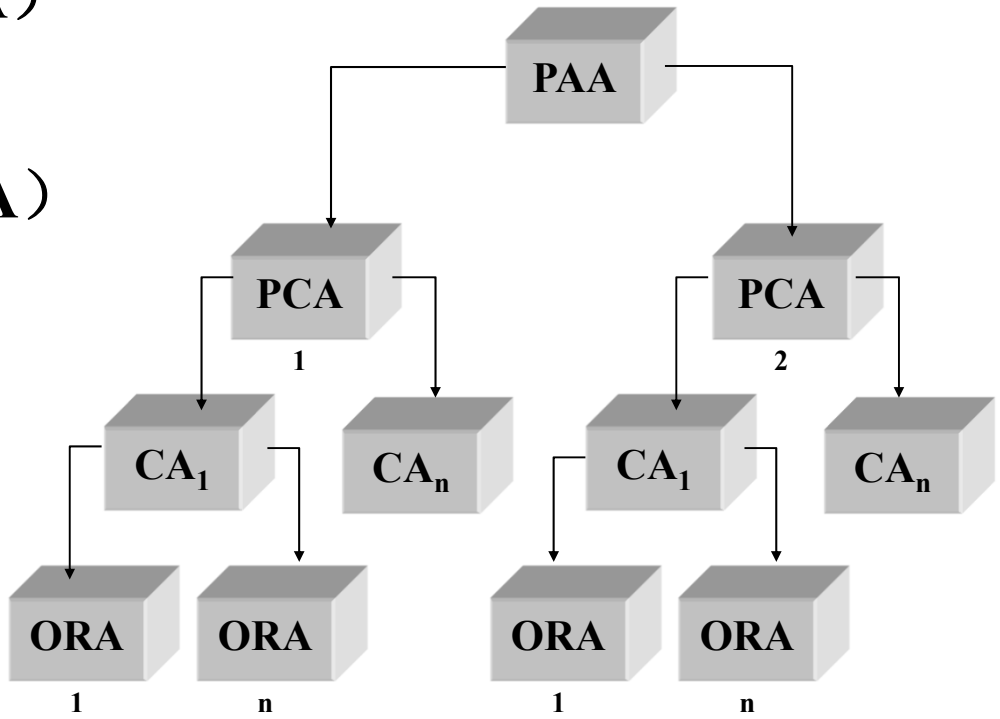
在传统的安全解决方案中，密码服务与应用紧密地结合在一起，每一种网络应用都有自己的一套密钥管理，功能大量冗余，管理维护工作复杂，费用高，而且这种分散式的方案存在安全隐患，互操作性也得不到保证；而PKI以统一的、通用的方式来解决所有应用的共同安全问题。利用PKI可以方便地建立和维护一个可信的网络计算环境，从而使得人们在这个无法直接相互面对的环境里，能够确认彼此身份和所交换的信息，能够安全地从事商务活动。



§6.3 公钥基础设施PKI

➢ 典型的PKI体系结构

- 策略批准机构（PAA）
- 策略控制机构（PCA）
- 认证机构（CA）
- 在线证书申请（ORA）



§6.3 公钥基础设施PKI

- PKI由一系列组件和服务构成：
  1、认证机构CA、注册机构RA
  2、证书库
  3、证书撤销
  4、密钥备份和恢复
  5、自动密钥更新
  6、密钥文档管理
  7、交叉认证
  8、支持不可否认
  9、时间戳
  10、客户端软件

§6.3 公钥基础设施PKI

1、认证机构CA (Certification Authority)

为信息安全提供有效的、可靠的保护机制，包括机密性、身份验证特性、不可否认性(交易的各方不可否认它们的参与)。这就需要依靠一个可靠的第三方机构验证，而认证机构CA专门提供这种服务。

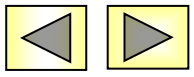
CA是PKI的关键组成部分。CA通过对一个包含身份信息和相应公钥的数据结构进行数字签名来捆绑用户的公钥和身份，这个数据结构被称为公钥证书（简称证书）。

§6.3 公钥基础设施PKI



CA的职能：

- 接收验证最终用户数字证书的申请。
- 确定是否接受最终用户数字证书的申请-证书的审批。
- 向申请者颁发、拒绝颁发数字证书-证书的发放。
- 接收、处理最终用户的数字证书更新请求-证书的更新。
- 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。
- 数字证书的归档。
- 密钥归档。
- 历史数据归档



§6.3 公钥基础设施PKI

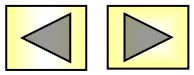


认证中心为了实现其功能，主要由以下三部分组成：

注册服务器：通过 Web Server 建立的站点，可为客户提供每日24小时的服务。因此客户可在自己方便的时候在网上提出证书申请和填写相应的证书申请表，免去了排队等候等烦恼。

证书申请受理和审核机构：负责证书的申请和审核。它的主要功能是接受客户证书申请并进行审核。

认证中心服务器：是数字证书生成、发放的运行实体，同时提供发放证书的管理、证书废止列表（CRL）的生成和处理等服务。



§6.3 公钥基础设施PKI

注册机构RA (Registration Authority)

由于一个PKI区域的最终实体数量的增加，RA可以充当CA和它的最终用户之间的中间实体，辅助CA来完成日复一日的证书处理功能。RA是CA的证书发放、管理的延伸，是整个CA中心得以正常运营不可缺少的一部分。

RA通常提供下列功能：

- 接收和验证新注册人的注册信息；
- 代表最终用户生成密钥；
- 接收和授权密钥备份和恢复请求；
- 接收和授权证书撤销请求；
- 按需分发或恢复硬件设备。

§6.3 公钥基础设施PKI

数字证书：

网络通讯中标志通讯各方身份信息的一系列数据，提供了一种在Internet上验证身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。由权威机构CA机构发行的，人们可以在交往中用它来识别对方的身份。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。

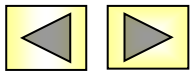
可用于：安全地发送电子邮件；访问安全站点、网上招投标、网上签约、网上订购、安全网上公文传送、 网上办公、网上缴费、网上购物等网上的安全电子事务处理和交易。

§6.3 公钥基础设施PKI

证书的获取：

- 发送者发送签名信息时，附加发送自己的证书；
- 单独发送证书信息的通道；
- 可从访问发布证书的目录服务器获得；
- 或者从证书的相关实体(如RA)处获得；

在PKI体系中，可以采取某种或某几种的上述方式获得证书。发送数字签名证书的同时，可以发布证书链。这时，接收拥有证书链上的每一个证书，从而可以验证发送者的证书。



§6.3 公钥基础设施PKI

证书的主要内容：

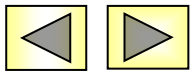
证书的格式与证书发放 数字证书格式的通用标准是**X.509**。根据该标准，数字证书应有下列信息：

版本号；序列号； 签字算法；发出该证书的认证机构；

有效期限；主体信息（包括持有人姓名、服务处所等信息）；

公共密钥信息； 认证机构的数字签字。

在**X.509**标准的扩展部分，认证机构可以说明该证书的附加信息，如密钥用途等。



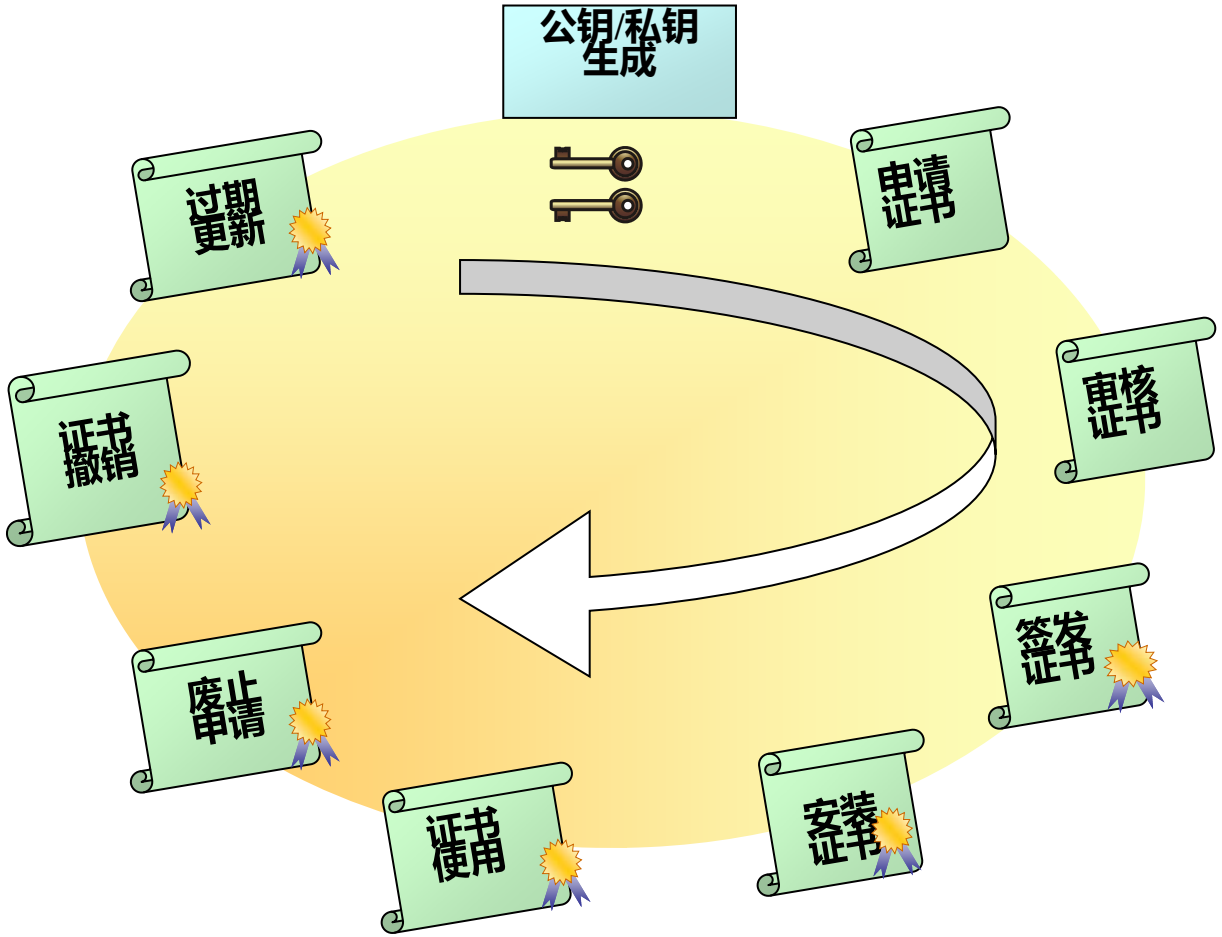
§6.3 公钥基础设施PKI

证书的管理：

- 用户能方便地查找各种证书及已经撤销的证书。
- 根据用户请求或其它相关信息撤销用户的证书。
- 能根据证书的有效期限自动地撤销证书。
- 能完成证书数据库的备份工作。
- 证书的管理通过目录服务来实现。

§6.3 公钥基础设施PKI

证书的生命周期：



§6.3 公钥基础设施PKI

证书的使用：

当用户向某一服务器提出访问请求时，服务器要求用户提交数字证书。收到用户的证书后，服务器利用CA的公开密钥对CA的签名进行解密，获得信息的散列码。然后服务器使用与CA相同的散列算法对证书的信息部分进行处理，得到一个散列码，将此散列码与对签名解密所得到的散列码进行比较，若相等则表明此证书确实是CA签发的，而且是完整性未被篡改的证书。这样，用户便通过了身份认证。服务器从证书的信息部分取出用户的公钥，以后向用户传送数据时，便以此公钥加密，对该信息只有用户可以进行解密。

§6.3 公钥基础设施PKI

挂起证书：

有时，CA需要临时限制证书的使用，但又不需要撤销证书。

例如，一个企业最终用户可能正在出差。在这种情况下，可以挂起（suspend）证书；这样就可以禁止使用那些带有PKI功能的应用程序，这些应用程序在该雇员不在的情况下是不能访问的。当该雇员返回时，CA清除该挂起。由于这种方法不需要先请求吊销证书然后再重新颁发证书，从而节省了CA的时间。为了挂起一个证书，CA在CRL原因代码扩展项中使用证书冻结值。

§6.3 公钥基础设施PKI

证书撤销：

CA签发的证书捆绑了用户的身份和公钥，在生命周期里都是有效的。但在现实环境中，由于这些原因包括：用户身份的改变、对密钥的怀疑（丢失或泄露）、用户工作的变动等。必须存在一种机制撤销这种认可，在PKI中这种机制被称为证书撤销。

证书撤销最常用的方式是使用证书废除列表CRL(Certificate Revocation List)，CRL是一种包含了撤销的证书列表的签名数据结构。它含有带时间戳的已撤销证书的列表。CRL的完整性和可靠性由它本身的数字签名来保证，通常CRL的签名者就是证书的签发者。当CRL创建并且被签名以后，就可以通过网络自由地分发，或以处理证书的同样方式存储在一个目录中。

§6.3 公钥基础设施PKI

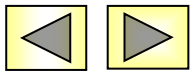


证书撤销的申请：

当PKI中某实体的私钥被泄漏时，被泄密的私钥所对应的公钥证书应被作废。

对CA而言，私钥的泄密不大可能，除非有意破坏或恶意攻击所造成；对一般用户而言，私钥的泄密可能是因为存放介质的遗失或被盗。

另外一种情况是证书中所包含的证书持有者已终止或与某组织的关系已经中止，则相应的公钥证书也应该作废。



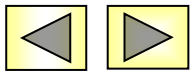
§6.3 公钥基础设施PKI



CRL的获取：

每一个CA均可以产生CRL，CRL可以定期产生也可以在每次有证书作废请求后，实时产生，CA应将其产生的CRL及时发布到目录服务器上去。

CRL的获取就可以有多种方式，CA产生CRL后，自动发送到下属各实体。大多数情况是由使用证书的各PKI实体从目录服务器获得相应的CRL。



§6.3 公钥基础设施PKI

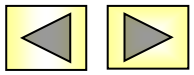


签名密钥对和加密密钥对：

（1）签名密钥对

签名密钥对由签名私钥和验证公钥组成。签名私钥具有日常生活中公章、私章的效力，为保证其唯一性，签名私钥绝对不能够作备份和存档，丢失后只需重新生成新的密钥对，原来的签名可以使用旧公钥的备份来验证。验证公钥需要存档，用于验证旧的数字签名。

用作数字签名的这一对密钥一般可以有较长的生命期。

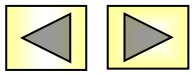


§6.3 公钥基础设施PKI

（2）加密密钥对

加密密钥对由加密公钥和解密私钥组成。为防止密钥丢失时丢失数据，解密私钥应该进行备份，同时还可能需要进行存档，以便能在任何时候解密历史密文数据。加密公钥无须备份和存档，加密公钥丢失时，只须重新产生密钥对。

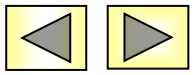
加密密钥对通常用于分发会话密钥，这种密钥应该频繁更换，故加密密钥对的生命周期较短。



§6.3 公钥基础设施PKI

（3）签名密钥对和加密密钥对的比较

这两对密钥的密钥管理要求存在互相冲突的地方，因此系统必须针对不同的用途使用不同的密钥对，尽管有的公钥体制算法，如目前使用广泛的**RSA**，既可以用于加密、又可以用于签名，在使用中仍然必须为用户配置两对密钥、两张证书，分别用于数字签名和加密。



§6.3 公钥基础设施PKI

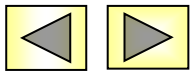


PKI系统的信任模型

选择适当的信任模型是构筑和运作**PKI**所必需的一个环节。选择正确的信任模型以及与它相应的安全级别是非常重要的，同时也是部署**PKI**所要做的较早和基本的决策之一。

信任模型主要阐述了以下几个问题：

- 一个**PKI**用户能够信任的证书是怎样被确定的？
- 这种信任是怎样被建立的？
- 在一定的环境下，这种信任如何被控制？



§6.3 公钥基础设施PKI

- 常用的四种信任模型：
  - （1）认证机构的严格层次结构模型
  - （2）分布式信任结构模型
  - （3） Web模型
  - （4）以用户为中心的信任模型

§6.3 公钥基础设施PKI

- **PKI的实施：**

  关键：商业驱动，而不是以技术为中心

  好处：安全电子邮件、安全电子数据交换EDI、安全电子表格、安全的企业内(外)部网、实体访问控制、安全远程访问、安全Web应用、客户签名、简化登录。

  提高工作效率、优化劳动力、减少风险、降低通信费用等。

- **PKI实施中的障碍：**
  - 资料库问题：缺少业界标准、多个生产厂家产品间的可互操作性、可升级性与性能
  - **PKI支撑的应用**
  - 专业人才