信息安全原理与技术

郭亚军　宋建华　李莉

清华大学出版社

第8章 公钥基础设施

- 主要知识点：
  - 公钥基础设施PKI（Public Key Infrasturcture）
  - 认证中心CA（Certificate Authority）
  - 数字证书（Digital Certificate）
  - 证书撤销链表CRL（Certificate Revocation Lists）
  - 在线证书状态协议OCSP（Online Certificate status Protocol）
  - 交叉认证(Cross-Certification)
  - 证书用户（Certificate User）
  - 简单认证（Simple Authentication）
  - 强认证（Strong Authentication）
  - X.509

PKI概念

- PKI是利用公钥密码理论和技术为网络安全应用提供安全服务的基础设施，不针对任何一种具体的网络应用，但它提供了一个基础平台，并提供友好的接口。
- PKI采用数字证书对公钥进行管理，通过第三方的可信任机构（认证中心，即CA），把用户的公钥和用户的其他标识信息捆绑在一起。
- 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的使用加密、数字签名技术等多种密码技术，从而保证网上数据的安全性。

PKI提供的安全服务

- 认证性：认证服务与保证通信的真实性有关。认证服务向接收方保证消息来自于所声称的发送方。认证性包括实体认证和数据源认证。
- 数据保密性：防止传输的信息收到被动攻击。
- 数据完整性：保证消息在通信中没有被攻击者篡改。
- 不可否认性：防止信息发送方或接收方否认传输或接受过某条消息。
- 访问控制：限制和控制通过通信连接对主机和应用进行存取的能力。

PKI涉及的密码技术（1）

- 对称和非对称加/解密
- 消息验证码与散列函数
- 数字签名

PKI涉及的密码技术（2）

- 对称和非对称加/解密
  - 对称加密机制也称单钥密码技术，即加密密钥和解密密钥是相同的。对称密码加密机制的特点是：保密性好，计算效率高，处理速度快，适合于大数据量的加/解密。但是缺点是：对于密钥的分发管理困难。
  - 非对称密码体制也称为公钥密码体制后双钥密码体制，它不仅可以提供加/解密功能，还可以实现数字签名。非对称密码机制的特点是：便于密钥的分发管理、可以实现数字签名。缺点是：计算上效率低，不适合大数据量的处理。

PKI涉及的密码技术（3）

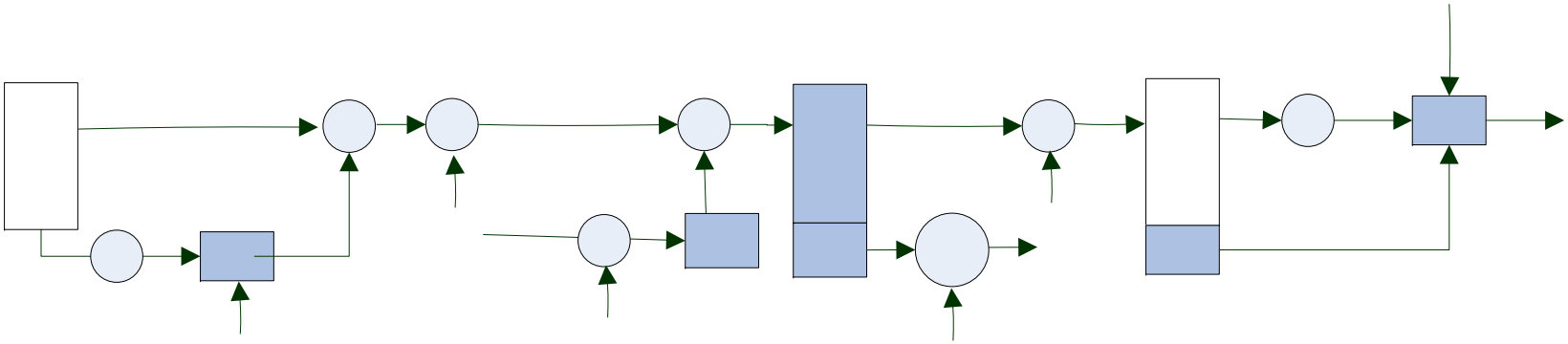
- 消息验证码与散列函数
  - 消息认证码是保证数据完整性的加密技术，它使用密钥对消息进行加密处理，生成一段短数据块，作为消息的认证码。提供数据的完整性服务。
  - 散列函数和消息认证码函数功能类似，也是对消息产生一段短的数据块，作为和原始消息相关的认证信息，但是不同的是散列函数不使用密钥信息。散列函数通常和非对称密码机制结合使用，用来实现数字签名

PKI涉及的密码技术（4）

- 数字签名
  - 直接使用签名私钥进行数字签名：这种方式适合于对数据量小的信息进行签名。
  - 结合散列函数实现数字签名：这种方式适合对数据量大的信息进行签名。首先对被签名的消息计算散列值，然后使用私钥对消息散列值而不是直接对消息进行签名。验证者收到消息及签名后，首先是使用散列函数计算出所收到的消息的散列值，然后使用公钥对该散列值以及收到的数字签名进行验证。

PKI涉及的密码技术（5）

- 数字信封

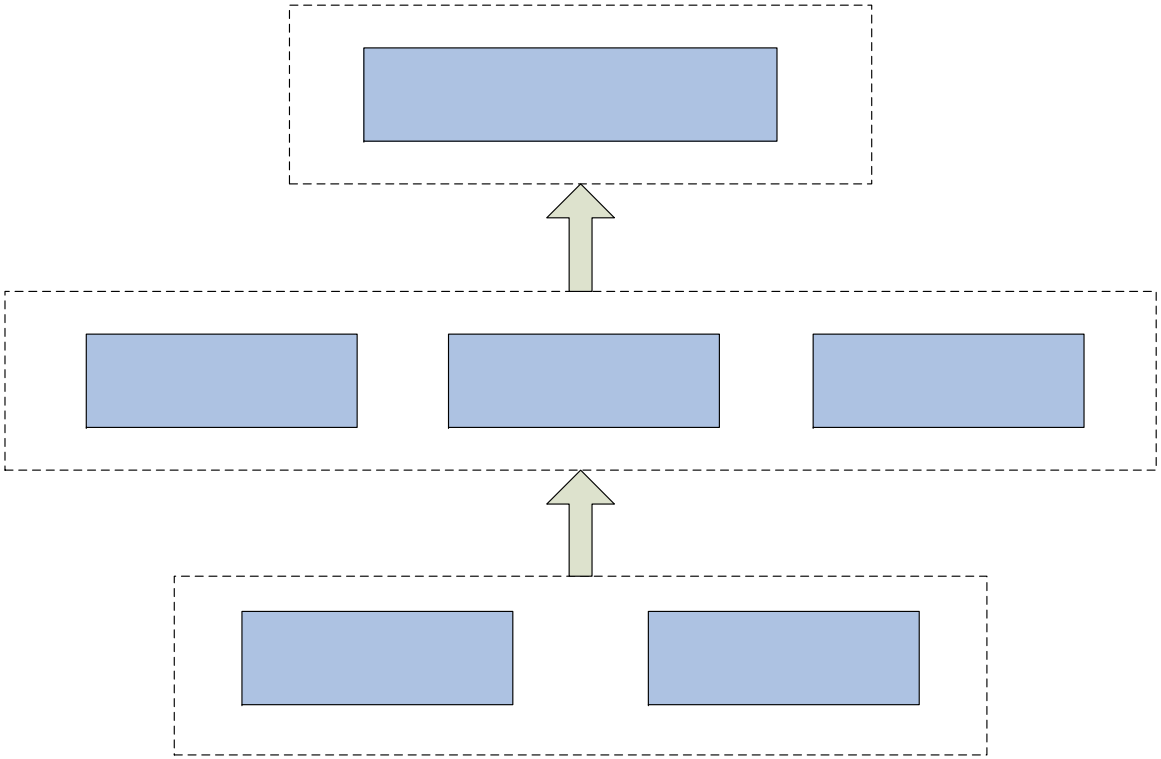


发送者A

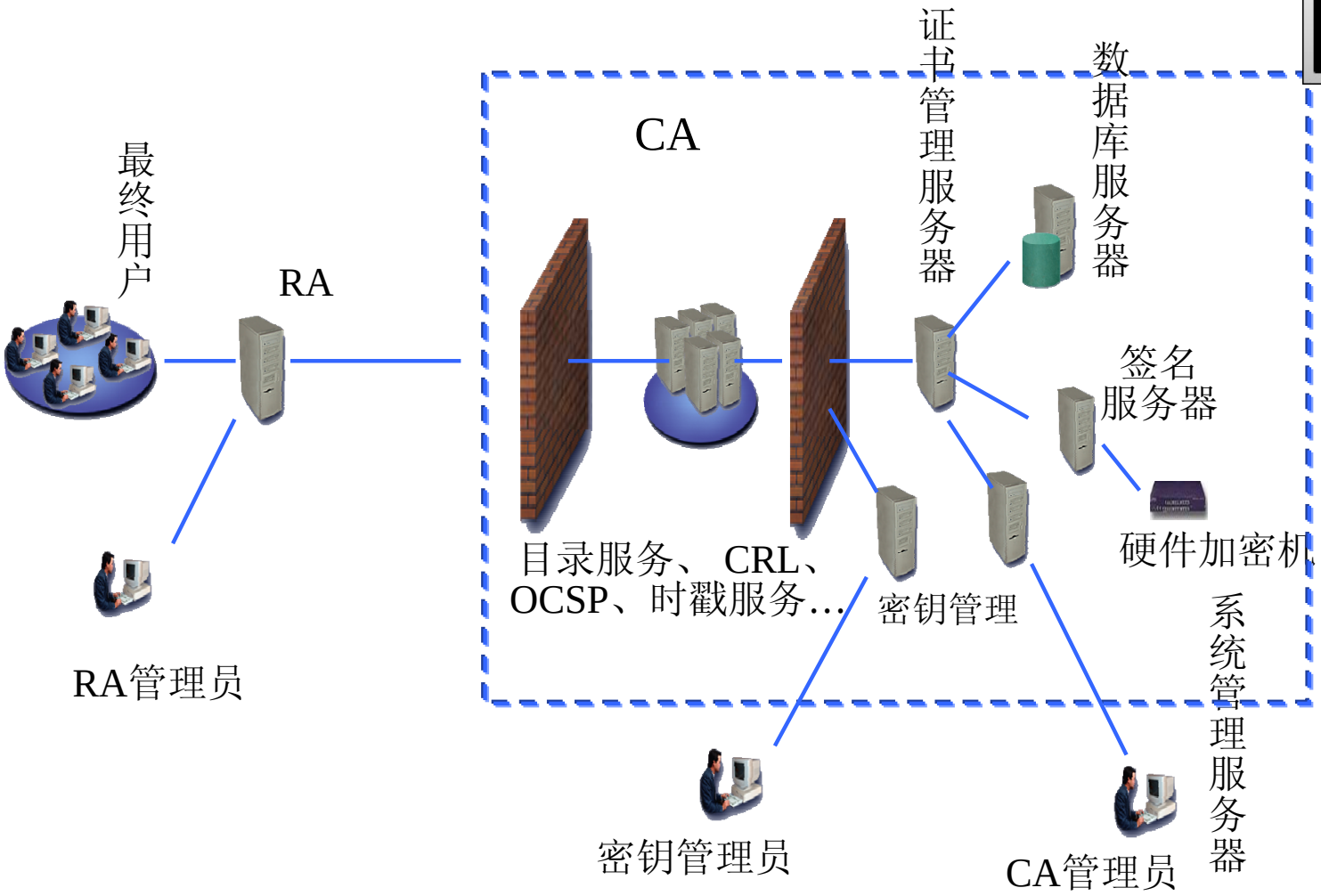
PKI涉及的密码技术（6）

- 双重数字签名
  - 所谓双重签名，是指发送者需要发送两组相关的信息给接收者，对这两组相关信息，接收者只能解读其中的一组，而另一组只能直接转发给第三方接收者。这种应用中使用的两组数字签名称为双重数字签名。

PKI组成



PK



PKI系统的构建必须包括认证机构、证书库、密钥备份及恢复系统、证书撤销系统、PKI应用接口等基本成分。

认证机构

- 认证机构CA是PKI的核心组成部分，是证书的颁发机构。
- 认证中心的任务就是负责产生、分配并管理数字证书。每一份数字证书都与上一级的数字签名证书相关联，最终通过安全链追溯到一个已知的并被广泛认为是安全、权威、足以信赖的机构-根认证中心（根CA）

认证机构的职责

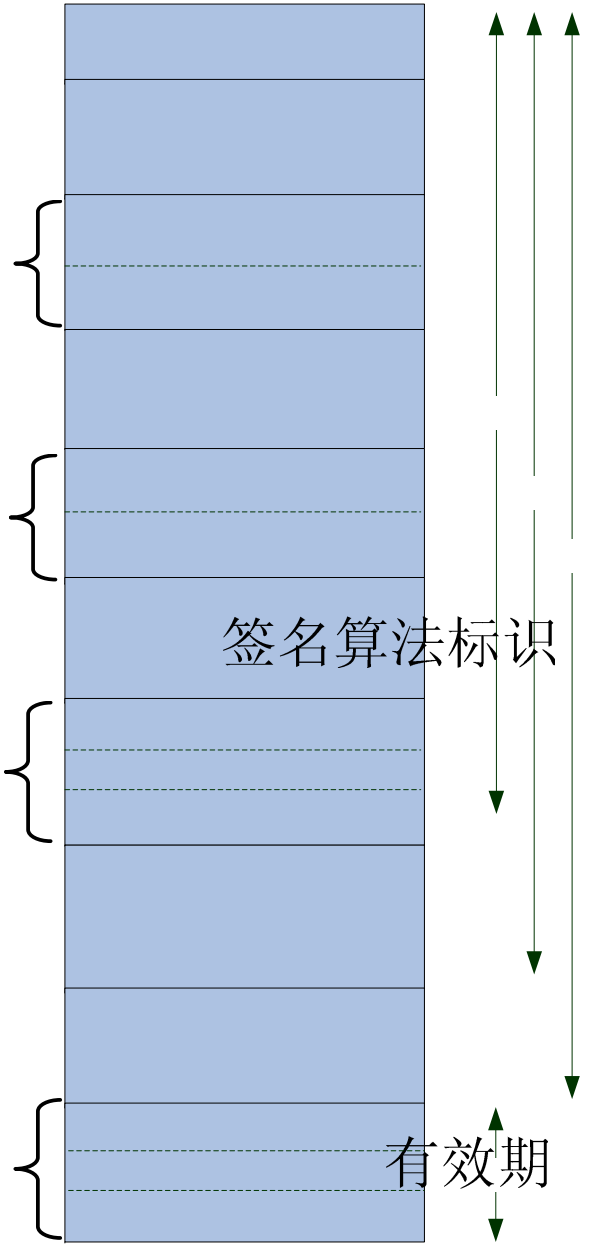
- 验证并标识证书申请者的身份；
- 确保CA用于签名证书的非对称密钥的质量；
- 确保整个认证过程的安全性，确保签名私钥的安全性；
- 证书资料信息（包括公钥证书序列号、CA标识等）的管理；
- 确定并检查证书的有效期；
- 确保证书主题标识的唯一性，防止重名；
- 发布并维护作废证书列表；
- 对整个证书签发过程做日志记录；
- 向申请人发出通知。

密钥对的生成

- 主体的公钥可以由如下方式产生，然后由CA对其进行数字签名：
  - 用户自己生成密钥对，然后将公钥以安全的方式传送给CA，这种方法的优点是用户私钥不会传播给其他实体，但该过程必须保证用户公钥的可验证性和完整性。
  - 密钥对由CA产生，然后将其以安全的方式传送给用户。认证机构是用户信任的实体，并且具有必要的、安全的安全手段，这是一种比较合适的选择。该过程必须确保密钥对待机密性、完整性和可验证性，这种方式对CA待可信性要求更高。

数字证书

- 数字证书也成为公钥证书、电子证书，是公钥体制中使用的公钥的一个密钥管理载体，它是一种权威性的电子文档，形同网络环境中的一种身份证，用以证明某个主题（如用户、服务器等）的身份以及其所持有的公开密钥的真实性和合法性。
- 证书是PKI的管理核心，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。证书的格式遵循ITUT X.509国际标准。



版本
Version

证书序列号
Certificate Serial Number

算法 algorithms

参数 parameters

签发者名字
Issuer Name

x.509 v3证书格式

生效日期 not before

失效日期 not after

证书库

- 证书库是CA颁发证书和撤销证书的集中存放地，是网上一种公共信息库，可供用户进行开放式查询。
- 证书库的通常构造方法是采用支持LDAP协议的目录系统。证书及证书撤销信息在目录系统上发布，其标准格式采用X.500系列。用户或相关应用可以通过LDAP来访问证书库，实时查询证书和证书撤销信息。系统必须保证证书库的完整性，防止伪造、篡改证书。

证书撤销

- 数字证书在有效期内可能因为一些原因需要撤销用户信息和公钥的捆绑关系。这就需要终止证书的生命期，并警告其他用户不再使用这个证书。
- PKI为此提供了证书撤销的管理机制，撤销证书有以下几种机制：
  - 撤销一个或多个主体的证书；
  - 撤销由某一对密钥签发的所有证书；
  - 撤销由CA签发的所有证书。

证书撤销-CRL

- 一般CA通过发布证书撤销列表CRL来发布撤销信息
  - CRL是由CA签名的一组电子文档，包括了被撤销证书的唯一标识（证书序列号）
  - CRL为应用程序和其它系统提供了一种检验证书有效性的方式
  - 任何一个证书被撤销后，CA会通过发布CRL的方式来通知各方

证书撤销-OCSP

- 对证书撤销信息的查询，也可以使用在线查询方式。在线证书状态协议（Online Certificate status Protocol，简称OCSP）是IETF颁布的用于检查数字证书在某一交易时间是否有效的标准，可以实时进行这类检查，比下载和处理CRL的传统方式更快、更方便和更具独立性。

密钥备份与恢复

- 可能很多原因造成丢失解密数据的密钥，那么被加密的密文将无法解开，造成数据丢失。为了避免这种情况的发生，PKI提供了密钥备份与解密密钥的恢复机制，即密钥备份与恢复系统。
- 在PKI中密钥的备份和恢复分为CA自身根密钥和用户密钥两种情况
- 值得注意的是，密钥备份和恢复一般只针对解密密钥，签名私钥是不做备份的。

PKI应用接口

- 完成证书的验证，为所有应用提供一致、可信的方式使用公钥证书；
- 以安全、一致的方式与PKI的密钥备份与恢复系统交互，为应用提供统一的密钥备份与恢复支持；
- 在所有应用系统中，确保用户的签名私钥始终在用户本人的控制下；
- 根据案情策略自动为用户更换密钥，实现密钥更换的自动、透明与一致；
- 为方便用户访问加密的历史数据，向应用提供历史密钥的安全管理服务；
- 为所有应用访问统一的公钥证书库提供支持；
- 以可信、一致的方式与证书撤销系统交互，向所有应用提供统一的证书撤销处理服务；
- 完成交叉证书的验证工作，为所有应用提供统一模式的交叉验证支持；
- 支持多种密钥存储介质；
- 提供跨平台服务。

PKI的功能

- 证书的管理
- 密钥的管理
- 交叉认证
- 安全服务

PKI的功能-证书的管理

- 证书的申请和审批
  - 用户从RA处获得申请表，填写相关内容，提交给RA，由RA对相关内容进行审核并决定是否审批通过该证书申请的请求。通过后RA将申请请求及审批通过的信息提交给相应的认证中心CA。
  - 证书的申请和审批方式有离线和在线两种

PKI的功能-证书的签发

- 证书的签发
  - RA完成了证书的申请和审批后，将证书请求提交给CA，由CA颁发所申请的证书，其中由CA所生成的证书格式符合X.509 V3标准，CA对证书进行数字签名。
  - 证书的发放分为离线方式和在线方式两种

PKI的功能-证书的查询和管理

- 证书的查询和获取
  - 当用户收到发送者进行数字签名的信息时，需要验证该数字签名，或希望加密信息发送给其他用户，需要获取其他用户的公钥证书并验证有效性。
- PKI体系中提供了获取证书的多种方式
  - 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处获得。

PKI的功能-证书的撤销

- 证书撤销
  - 证书在使用过程中可能会因为各种原因而被废止，例如：密钥泄密，相关从属信息变更，密钥有效期中止或者CA本身的安全隐患引起废止等。
  - CRL和OCSP

PKI的功能-密钥的管理

- 密钥的产生和分发
  - 用户公/私钥对的产生、验证及分发有两种方式：用户自己产生或由代理产生
- 密钥的备份和恢复
  - CA自身根密钥和用户密钥两种情况
- 密钥的自动更新
- 密钥历史档案管理

PKI的功能-交叉认证

- 每个CA只能覆盖一定的作用范围，这个范围成为CA的域，当属于不同CA域的用户需要进行安全通信时，则需要提供一种互相认可对方证书的机制，在原本没有联系的CA之间建立信任关系，这就是交叉认证(Cross-Certification)。

PKI的功能-交叉认证

- 交叉认证从CA所在域来分有两种形式：
  - 域内交叉认证和域间交叉认证。域内交叉认证即进行交叉认证的两个CA属于相同的域
  - 完全独立的两个组织间的CA之间进行交叉认证就是域间交叉认证。
- 交叉认证有两个操作：
  - 首先在两个域之间建立信任关系。每个CA签发一张包含自己公钥的证书，该证书称为交叉证书。
  - 后续操作由客户端软件完成，这个操作包含了验证已由交叉认证的CA签发的用户证书的有效性。

PKI的功能-安全服务

- 身份认证
- 完整性
- 机密性
- 不可否认性
- 时间戳
- 数据的公正性服务

安全服务-身份认证

- 身份认证指的是用户提供他是谁的证明。认证的实质就是证实被认证对象是否属实和是否有效的过程，常常被用于通信双方相互确认身份，以保证通信的安全。其基本思想是通过验证被认证对象的某个专有属性，达到确认被认证对象是否真实、有效的目的。PKI的认证服务采用数字签名这一密码技术。

安全服务-身份认证（2）

- 作为认证体系的PKI，完成身份认证主要体现在以下所述的3个步骤和层次。
  - 交易双方建立连接后，首先一方验证另一方所持证书的有效性，通过访问证书目录，查询各自的证书撤销列表，以确认各自的证书都是当前使用的有效证书。
  - 交易一方验证另一方所持证书是否为共同认可的可信CA签发，即CA的有效性。
  - 完成了以上的验证，证书的有效性得到了确认。在真正处理业务前，交易中的被验证一方还要对一些可以验证身份的信息，如自己的标识符和口令用所拥有的签名私钥进行签名，然后传给该交易中的验证一方。这时验证方就可以直接用被验证方的证书中的公钥对这次所做的签名进行验证。

安全服务-数据完整性

- 数据的完整性就是防止对信息的非法篡改，确通信双方接收到的数据和从数据源发出的数据完全一致。
- 可以通过采用安全的散列函数和数字签名技术实现数据完整性保护，特别是双重数字签名可以用于保证多方通信时数据的完整性。

安全服务-数据机密性

- 数据的机密性就是实现对所保护数据的加/解密，从而保证数据在传输和存储中，非授权的人无法获取真实的信息。所有的机密数据都是由加密技术实现的。而PKI的机密性服务是一个框架结构，通过这个功能模块可以实现交易中的算法协商和密钥交换，而且对参与通信的实体来说这些过程是透明的。

安全服务-不可否认性

- 不可否认用于从技术上保证实体对他们行为的诚实，即参与交互的双方都不能事后否认自己曾经处理过的每次操作。这在电子商务、电子政务等应用中非常重要，主要包括：数据来源的不可否认性、发送方的不可否认性，以及接收方在接收后的不可否认性。PKI所提供的不可否认功能，是基于数字签名，以及其所提供的时间戳服务功能的。

安全服务-时间戳

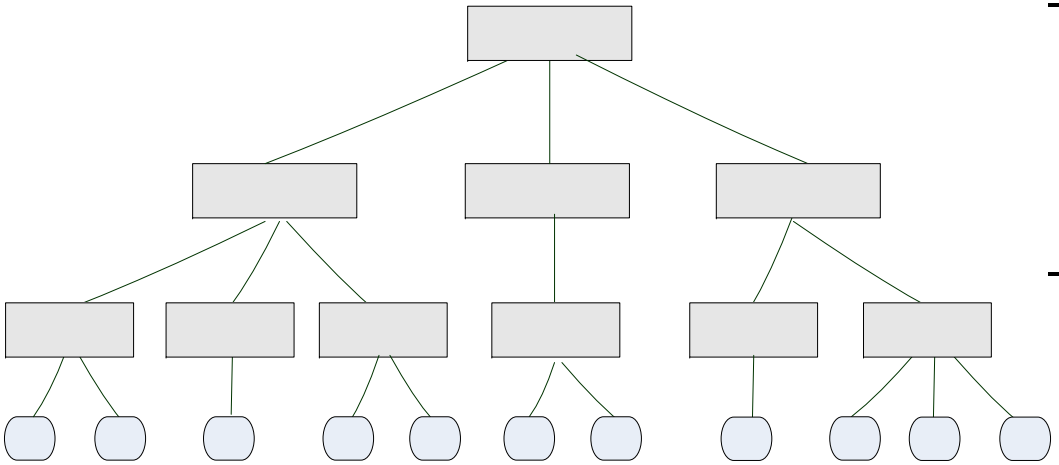
- PKI中的时间戳机构（TSA，Time Stamp Authority）可以提供时间戳服务，给电子文档加上权威的时间凭证。
- PKI中必须存在用户可信任的权威时间源（事实上，权威时间源提供的时间并不需要正确，仅仅需要用户作为一个“参照”时间完成基于PKI的事务处理。
- 虽然安全时间戳是PKI支撑的服务，但它依然可以在不依赖PKI的情况下实现安全时间戳服务。一个PKI体系中是否需要实现时间戳服务，完全依照应用的需求来决定。

信任模型

- 所谓信任模型就是一个建立和管理信任关系的框架。信任模型描述了如何建立不同认证机构之间的认证路径以及构建和寻找信任路径的规则。
- PKI的信任模型主要阐述以下一些问题：
  - 一个实体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？
- 目前较流行的PKI信任模型主要有四种：认证机构的严格层次结构模型、分布式信任结构模型、Web模型、以用户为中心的信任模型。

信任模型-认证机构的严格层次结构

- 认证机构的严格层次结构可以描绘为一棵倒转的树，根在顶上，叶在最下面。



– 根代表一个对整个PKI域内的所有实体都有特别意义的CA，被叫做根CA，作为信任的根或“信任锚”。
– 在根CA 的下面是零层或多层中间CA（也被称作子CA，它们是从属于根CA）。
– 与非CA 的PK实体相对应的叶节点通常被称作终端实体或终端用户。

根CA

信任模型-认证机构的严格层次结构（2）

- 根CA具有一个自签名的证书，依次对它下面的CA进行签名；层次结构中叶子节点上的CA用于对终端实体进行签名；对于实体而言，它信任根CA，可以不必关心中间的CA；但它的证书是由底层的CA签发的。要维护这棵树，在每个节点CA上需要保存两种证书：
  - (1) 向前证书（Forward Certificates）：其他CA发给它的证书；
  - (2) 向后证书（Reverse Certificates）：它发给其他CA的证书。

信任模型-认证机构的严格层次结构（3）

- 假设实体A收到B的一个证书，B的证书中含有签发该证书的CA的信息，沿着层次树往上找，可以构成一条证书链，直到根证书。验证过程正好沿相反的方向，从根证书开始，依次往下验证每一个证书中的签名，一直到验证B的证书中的签名。如果所有的签名验证都通过，则A可以确定所有的证书都是正确的，如果他信任根CA，则他可以相信B的证书和公钥。

信任模型-分布式信任结构

- 与严格层次结构相反，分布式信任结构把信任分散到两个或更多个CA 上。更准确地说，A 把CA1的公钥作为他的信任锚，而B可以把CA2 的公钥做为他的信任锚。因为这些CA 的密钥都作为信任锚，因此相应的CA 必须是整个PKI群体的一个子集所构成的严格层次结构的根CA (CA1：是包括A 在内的层次结构的根，CA2是包括B 在内的层次结构的根）。
- 如果这些严格层次结构都是可信颁发者层次结构,那么该总体结构被称作完全同位体结构(fully peered architecture)
- 一般说来,完全同位体结构部署在某个组织内部，而满树结构和混合结构则是在原来相互独立的PKI系统之间进行互联的结果。在不同的同位体根CA之间的互连过程则保被称为交叉认证。

信任模型-Web 模型

- Web模型是在WWW上诞生的，依赖于流行的浏览器进行构建。在这种模型中，许多CA的公钥被预装在标准的浏览器上。这些公钥确定了一组浏览器用户最初信任的CA。
- Web模型在方便性和简单互操作性方面有明显的优势,但是也存在许多安全隐患。
  - 因为浏览器的用户自动地信任预安装的所有公钥，所以即使这些根CA中有一个是有问题的，安全性将被完全破坏。
  - 没有实用的机制来撤销嵌入到浏览器中的根密钥。
  - 该模型还缺少在CA和用户之间建立合法协议的有效方法

信任模型-以用户为中心的信任模型

- 在一般被称作以用户为中心的信任模型中，每个用户都对决定信赖哪个证书和拒绝哪个证书直接完全地负责。在这个信任模型中，没有专门的CA中心，每个用户可以向他所信任的人签发公钥证书，通过这样的方式建立一个信任网。
- 以用户为中心的模型在技术水平较高和利害关系高度一致的群体中是可行的，但是在一般的群体（其用户有极少或者没有安全及PKI的概念）中是不现实的。
- PGP（Pretty Good Privacy）使用的就是以用户为中心的信任模型。

PKI的相关标准

- X.209ASN.1基本编码规则
- **X.500**
- X.509
- PKCS系列标准
- LDAP 轻量级目录访问协议

PKI的相关标准-X.209ASN.1

- ASN.1是描述在网络上传输信息格式的标准方法。
  - 第一部份（ISO 8824/ITU X.208）描述信息内的数据、数据类型及序列格式，也就是数据的语法；
  - 第二部分（ISO 8825/ITU X.209）描述如何将各部分数据组成消息，也就是数据的基本编码规则。

PKI的相关标准-X.500

- X.500是一套已经被国际标准化组织（ISO）接受的目录服务系统标准，它包括了一系列完整的目录数据服务，定义了一个机构如何在全局范围内共享其名字和与之相关的对象。
- X.500是层次性的，其中的管理域（机构、分支、部门和工作组）可以提供这些域内的用户和资源信息。它定义一个机构如何在一个企业的全局范围内共享名字和与它们相关的对象。
- 在PKI体系中，X.500被用来惟一标识一个实体，该实体可以是机构、组织、个人或一台服务器。X.500被公认为是实现一个目录服务的最好途径，但是它的实现需要很大投资，效率不高，在实际应用中存在着不少障碍。鉴于此，出现了DAP的简化版LDAP。

PKI的相关标准-X.500

- 总结而言，X.500所规定的目录服务有以下特点：
  - 分布性
  - 灵活性
  - 查询灵活
  - 平台无关
  - 全球统一的名字空间
  - 安全性

PKI的相关标准-X.509

- X.509是由国际电信联盟制定的数字证书标准。在X.500确保用户名称唯一性的基础上，X.509为X.500用户名称提供了通信实体的认证机制，并规定了实体认证过程中广泛适用的证书语法和数据接口。
- PKI是在X.509基础上发展起来的。X.509标准的范围包括下面四个方面：
  - 具体说明了目录的认证信息的形式；
  - 描述如何从目录获取认证信息；
  - 说明如何在目录中构成和存放认证信息的假设；
  - 定义各种应用使用的认证消息执行的方法。

PKI的相关标准-X.509（2）

- X.509标准中描述了两种认证
  - 简单认证(使用口令作为身份的认证)
  - 强认证（使用密码技术实现认证）

PKI的相关标准-X.509（3）

- 简单认证
  - 第一种方法是以清楚明确（即无保护）的方法将用户的可标识符和口令传送给接收方，其处理过程如下：
    - 发送方A将其标识符和口令发送给接收方用户B。
    - 用户B将用户A声明的标识符和口令发送给目录，然后目录用比较操作，检查与用户A有关的目录项的用户口令。
    - 目录向用户B返回证实（或否认）该口令是否有效的信息。
    - B可以向用户A发送认证结果，即成功或失败信息。
  - 第二种方法是将用户的标识符、口令，以及一个随机数和/或时间标记通过使用单向函数进行保护并传送。
  - 第三种方法是将第二种方法连同一个随机数和/或时间标记一起通过使用单向函数进行保护，然后再传送。

PKI的相关标准-X.509（4）

- 强认证
  - 单向认证

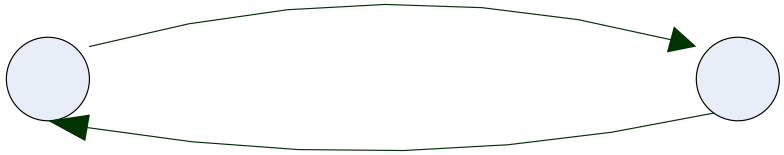
  - 其中，t_A是时间戳，r_A是随机数，sgnData是一个附加信息，为由签名者提供的数据源认证。A使用自己的私钥对这些信息进行数字签名。B收到后首先验证签名是否合法，再通过检查t_A,和r_A来判断该消息是否是重放消息。

$$A\{t_A, r$$

$$A$$

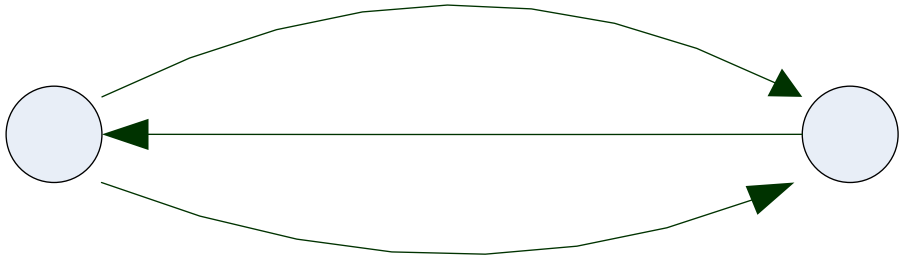
PKI的相关标准-X.509（5）

- 强认证
  - 双向认证



PKI的相关标准-X.509（6）

- 强认证
  - 三向认证



PKI的相关标准-PKCS系列标准

- 公钥密码标准（Public Key Cryptography Standard，简称PKCS）
  - PKCS#1：定义RSA公开密钥算法加密和签名机制
  - PKCS#3：定义Diffie-Hellman密钥交换协议。
  - PKCS#5：基于口令的加密标准。
  - PKCS#6：描述了公钥证书的标准语法，主要描述X.509证书的扩展格式。
  - PKCS#7：定义一种通用的消息语法
  - PKCS#8：描述私钥信息格式
  - PKCS#9：定义一些用于PKCS#6证书扩展、PKCS#7数字签名和PKCS#8私钥加密信息的属性类型。
  - PKCS#10：描述证书请求语法。
  - PKCS#11：定义了一套独立于技术的程序设计接口
  - PKCS#12：描述个人信息交换语法标准
  - PKCS#13：椭圆曲线密码体制标准。
  - PKCS#14：伪随机数生成标准。
  - PKCS#15：密码令牌信息格式标准

PKI的相关标准- **LDAP** 轻量级目录访问协议

- LDAP（Lightweight Directory Access Protocol）已经成为目录服务的标准，它比X.500 DAP协议更为简单实用，而且可以根据需要定制
  - （1）可以在任何计算机平台上，用很容易获得的而且数目不断增加的LDAP的客户端程序访问LDAP目录，而且也很容易定制应用程序为它加上LDAP的支持。
  - （2）LDAP协议是跨平台的和标准的协议，因此应用程序就不用为LDAP目录放在什么样的服务器上操心了。因为LDAP是Internet的标准，得到了业界的广泛认可和支持。LDAP服务器可以是任何一个开发源代码或商用的LDAP目录服务器（或者还可能是具有LDAP界面的关系型数据库），因为可以用同样的协议、客户端连接软件包和查询命令与LDAP服务器进行交互。大多数的LDAP服务器安装起来很简单，也容易维护和优化。

PKI的相关标准- **LDAP** 轻量级目录访问协议（2）

- LDAP （ Lightweight Directory Access Protocol）已经成为目录服务的标准，它比X.500 DAP协议更为简单实用，而且可以根据需要定制
  - （3）LDAP服务器可以用“推”或“拉”的方法复制部分或全部数据。LDAP服务器中内置了复制技术，且很容易配置。
  - （4）LDAP允许根据需要使用访问控制信息ACL控制对数据读和写的权限。
  - （5）LDAP提供了复杂的不同层次的访问控制或者ACL。这些访问可以在服务器端控制，因此比用客户端软件更能保证数据安全。

PKI的应用

- 虚拟专用网络（VPN）
  - 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，利用网络层安全协议（尤其是IPSec）和建立在PKI上的加密与签名技术来获得机密性保护。基于PKI技术的IPSec协议现在已经成为架构VPN的基础，它可以为路由器之间、防火墙之间或者路由器和防火墙之间提供经过加密和认证的通信。虽然它的实现复杂一些，但其安全性比其他协议都完善得多。在基于PKI对VPN产品中，用户使用数字证书在客户端和服务器之间建立安全的VPN连接。

PKI的应用

- 安全电子邮件
  - 实际使用中，PGP技术在电子邮件通信中得到了一定的发展，但由于PGP的应用模式局限了其应用是用户对用户的，并需要在通信之前实现沟通，对于电子邮件的安全需求（机密、完整、认证和不可否认）可以考虑采用PKI技术来获得。目前发展很快的安全电子邮件协议是S/MIME (The Secure Multipurpose Internet Mail Extension)的实现是依赖于PKI技术的。

PKI的应用

- Web安全
  - 基于PKI技术，结合SSL协议和数字证书，则可以保证Web交易多方面的安全需求，使Web上的交易和面对面的交易一样安全。

PKI的应用

- 安全电子交易（SET）
  - 由于SET提供了消费者、商家和银行之间的认证，确保了交易数据的安全性、完整可靠性和交易的不可否认性，因此它成为了目前公认的信用卡/借记卡的网上交易的国际安全标准。SET协议采用公钥密码体制和X.509数字证书标准，是PKI框架下的一个典型实现，同时也在不断升级和完善。

PKI的发展

- PKI发展的一个重要方面就是标准化问题，它也是建立互操作性的基础。
- PKI的发展受到应用驱动的影响，发展非常快，已经出现了大量成熟技术、产品和解决方案，正逐步走向成熟。
- 国内是从20世纪90年代末开始发展PKI及其应用，在此期间，PKI的厂商在PKI的可用性和技术实施方面也取得了很大进步。国内已经成功建设大型的行业性或是区域性的PKI/CA就有四十多个。