ch11 公钥基础设施

数字证书 page1

虽然证书只包含了公钥，但必须与对应私钥配合使用

数字证书和私钥的关系有点像锁和钥匙的关系。虽然锁里面没有包含钥匙，但是锁必须和钥匙配合使用

认证机构的私钥对散列值签名

数字证书的四种基本安全功能：身份认证，保密性，完整性，抗抵赖性 书page368

PKI 体系结构的组成 P9

证书是由机关、学校、团体等发的证明资格或权力的文件，是表明（或帮助断定）事理的凭证。

数字证书是包含用户身份信息、公钥以及CA数字签名的数据文件。主体将其身份信息和公钥以提交给CA认证中心，CA用自己的私钥对主体公钥和身份ID进行签名，生成由公钥、身份ID和CA签名三部分组成的证书。

利用数字证书进行加密和签名，也可以同时进行 P13~15

X.509证书格式 page17

保证公钥真实性 P19

公钥的分发虽然不需要保密，但需要保证公钥的真实性

就好像银行的客服电话，虽然不需要保密，但需要保证真实性

数字证书和公钥基础设施PKI就是为了实现在公钥分发过程中确保公钥真实性

PKI 作用 P20~22

公钥基础设施（Public Key Infrastructure）以公钥技术为基础，提供具有普适性安全服务的基础设施。PKI 旨在从技术上解决网上身份认证、信息的完整性和不可抵赖性等安全问题。

PKI基本功能：用户注册，证书申请，密钥产生，密钥更新，密钥备份，密钥恢复，证书作废，证书归档

PKI体系通常由终端实体用户、证书认证机构(CA)、证书注册机构(RA)和证书数据库，以及安全服务器组成

CA P23~25

证书机制是目前被广泛采用的一种安全机制，使用证书机制的前提是建立认证中心(CA)以及配套的注册中心(RA)系统。证书依靠一个可靠的第三方机构验证，CA专门提供这种服务。

产生自身证书并传输给安全服务器；验证用户的身份，产生、分配并管理PKI结构下的所有用户的证书；核心功能就是发放和管理数字证书；负责用户证书的黑名单登记和发布。

CA 的组成： 1 注册服务器 2 证书申请受理和审核机构 3 认证中心服务器 P25

RA P28

注册中心RA系统负责证书申请者的信息录入、审核以及证书发放等工作；对发放的证书完成相应管理功能

证书库 P29

证书集中存放地，用户可以从此处获得其他用户的证书和公钥；证书数据库服务器用于认证机构中数据（如密钥和用户信息等）、日志和统计信息的存储和管理。

安全服务器 P30

安全服务器面向普通用户，提供证书申请、浏览、撤销列表及证书下载等安全服务；用户首先得到安全服务器证书（CA颁发），然后用户与服务器之间的所有通信均以安全服务器的密钥进行加密传输，通过安全服务器的私钥解密得到明文，**保证了证书申请和传输过程中的信息安全性。**

密钥备份和恢复系统 P31

为防止用户丢失密钥或密钥被破坏，PKI提供解密密钥的备份和恢复的机制。解密密钥的备份和恢复由CA、专用备份服务器等可信机构完成。用于签名和校验的密钥对不可备份。

证书撤销列表 P32

私钥泄露、密钥更换、用户变化等情况，证书需要被注销，PKI中通过CA维护一个证书撤销列表（Certificate Revocation List，CRL）。检查CRL的URL应该内嵌在用户的证书中，可通过安全途径（SSL）访问URL，返回注销状态信息。

作废一个或多个主体的证书；作废由某一对密钥签发的所有证书；作废由某CA签发的所有证书。

PKI 应用接口系统 P33

PKI需要良好的应用接口系统，确保所建立起来的网络环境可信性，降低管理维护成本，向应用系统屏蔽密钥管理细节，提供证书验证及备份恢复。

CA 的信任关系 P34

信任、信任度、信任锚、信任域、信任模式。

PKI 信任模式 P35~36

PKI信任模型：证书用户、证书主体、各CA间的证书认证关系称为PKI信任模型。信任模型提供了建立和管理信任关系的框架，按照有无第三方可信机构参与，信任可划分为直接信任和第三方信任。第三方信任是指两个实体以前没有建立起信任关系，第三方为两者的可信任性进行了担保，是目前网络安全中普遍采用的信任模式。

CA 的层次结构 P37

对于大型权威机构，签发证书的工作不能仅仅由一个CA来完成，可建立一个CA层次结构。一个CA一般为一个安全域（security domain）的有限群体发放证书。每个CA覆盖一定作用范围，不同用户群体往往拥有不同的CA。

CA的信任模型 P38

1. 单CA信任模型：基本信任模型，也是目前许多组织或单位在Intranet中普遍使用的一种模型
2. 层次信任模型：层次信任模型也称为分级信任模型，它是一个以主、从CA关系建立的分级PKI结构
3. 分布式信任模型：分布式信任模型也称为网状信任模型，在这种模型中CA间存在着交叉认证
4. 桥CA的信任模型：桥CA信任模型也称为中心辐射式信任模型，被设计成用来克服层次信任模型和分布式信任模型的缺点，并连接不同的PKI系统。
5. WEB信任模型：Web信任模型构建在Web浏览器的基础上，浏览器厂商在浏览器中内置了多个根CA，每个根CA相互间是平行的，浏览器用户同时信任多个根CA并把这些根CA作为自己的信任锚。Web信任模型通过与相关域进行互连而不是扩大现有的主体群来使用户实体成为在浏览器中所给出的所有域的依托方。

严格层次结构模型 P40~42

CA的严格层次结构可描绘为一颗倒挂的树, 根代表整个系统信任起始点，是整个系统的信任锚,根CA下面的分支节点代表中间CA，被称作子CA，叶子节点代表终端用户。

认证过程：用户甲沿着CA的信任路径验证用户乙证书的数字签名，证书路径长度平均只有层次树高的一半

缺点：小规模群体容易对公共根CA达成一致信任，全局范围难以达成一致信任

建立过程 P41

验证过程 P42

层次模型的优缺点 P45

管理开销小；可扩展性好；与组织内部结构比较吻合；公共信任锚简化CA证书分发；实体到信任锚的路径固定。

只存在一个根CA作为公共信任锚，世界范围内不可能只有单个根CA；商业和贸易等信任关系不必采用层次型结构；根CA私钥的泄露的后果非常严重。

分布式信任模式 P46

分布式信任模型是一种 “对等模型”，建立信任的两个认证机构是对等关系。模型中CA间存在着交叉认证。信任针分散到两个或更多根 CA ，单CA安全性削弱不会影响整个PKI。

交叉验证 P47~48

交叉认证：是一种将以前无关的CA连接在一起的机制，认证主体和颁发者都是CA，根据CA是否属于同一信任域，分为域内交叉认证和域间交叉认证。

优点：灵活，便于建立特殊信任关系，符合商贸中双边信任关系；合理，PKI用户至少要信任其证书颁发CA；高效，频繁通信的CA间直接认证，降低 认证路径处理量；可靠，CA私钥泄露仅涉及到该CA的证书用户。

缺点：认证路径搜索策略可能很复杂；用户仅提供单个认证路径不能保证PKI的所有用户能验证他的签名。

桥 CA 信任模型 P49

中心辐射式信任模型；克服层次信任模型和分布式信任模型的缺点，连接不同的PKI系统。

Web CA 信任模式 P50 & P54

Web信任模型构建在Web浏览器的基础上，浏览器中内置多个根CA；根CA间是平行的，浏览器用户同时信任多个根CA并把这些根CA作为自己的信任锚。

实现方式：Web信任模型通过与相关域进行互连而不是扩大现有 的主体群来使用户实体成为在浏览器中所给出的所有 域的依托方

模型特点：具有分布式信任结构模型的特点，但根本上更类似于 认证机构的严格层次结构模型

认证形式：浏览器厂商起到了根 CA 的作用，而与被嵌入的密钥相 对应的CA就是它所认证的CA

安全隐患：预装公钥信任问题，用户自动地信任预装公钥，即使这些 CA 中有一 个是从没有认真核实被认证的实体，这时安全性将被完全破坏。缺乏根密钥撤销机制，没有实用的机制来撤销嵌入到浏览器中的根密钥。

以用户为中心的信任模式 PGP P56

由每个用户自己决定信任哪些证书。Pretty Good Privacy (PGP) 中，用户通过担当 CA（签署其他实体的公钥）和使其公钥被其他人认证建立 “信任网（Web of Trust）。当 A 收到一个属于 B 的证书时，发现这个证书由不认识的 D 签署的，但是 D 的证书是由 A 认识且信任的 C 签署，于是 A 决定信任 B 的密钥，也可决定不接受 B 的密钥。

PKI 安全问题 P59

1. 数字证书颁发过程中的安全问题：证书的合法性难以保证，误发证书，恶意颁发证书，钓鱼网站证书
2. 数字证书维护过程中的安全问题：证书的有效性难以验证，证书过期，证书撤销

PKI 证书撤销 P63

- 私钥泄露、密钥更换、用户变化时，需要 撤销证书
- CA 维 护 CRL (Certificate Revocation List ），末到期但已撤销证书列表
- 检查CRL的URL内嵌在用户证书，浏览器 安全访问URL查询证书状态, 确定是否被 CA 撤销
- 在线证书状态协议 OCSP (online certificate status protocol)是CRL之外维护PKI证书安全的另一个协议

中心化监督带来的问题 P64

证书的所有操作权利均归CA所有，在CA受到攻击后会带来严重的安全威胁；中心化监管导致PKI面临中心节点的安全脆弱性和信任链失效。

PKI安全问题的解决思路 P66

监督机制：证书透明机制；经济激励机制。

建立证书状态日志：证书撤销列表；在线证书状态；证书区块链。

建立监督机制 P67~68

证书透明机制：利用公开的证书状态日志来记录证书签发，撤销情况；CT服务器存储所有注册证书供第三方审计；解决证书合法性、有效性验证问题；容灾性较差，主要用于事后检测，提供追责证据。

经济激励机制：监督CA恶意证书的发布，检测者检查并上报，成功发现后扣除CA保证金奖励检测者/赔偿受害用户

建立证书状态日志 P69

证书撤销列表	在线证书状态	证书区块链
每个CA维护一个证书撤销列表 (Certificate RevocationList，CRL) 记录被撤销证书	用户通过CA指定在线证书状态服务器来查询证书的撤销状态信息	基于区块链记录证书的操作记录，维护最新的证书状态信息

证书撤销列表 P70

由CA 维护，包含被撤销的证书序列号和吊销时间；浏览器定期下载CRL列表用于校验证书是否已被撤销；CRL会越来越大，查询检验效率低；CRL实时性较差，证书被吊销后，服务器在更新 CRL 前依然信任证书。

在线证书状态 P71

在线证书状态协议（Online Certificate Status Protocol，OCSP），通过建立一个可实时响应的机制，CA服务器实时响应验证证书。OCSP要求浏览器直接请求第三方CA以确认证书的有效性，因此会损害隐私。客户端会在SSL中实时查询OCSP接口，获得查询结果前阻塞后续流程，降低HTTPS性能。

证书区块链 P72

利用去中心化技术，实现资源的可信保障，避免中心化带来的安全隐患，保证基础设施的安全可信。

系统安全性强：单一节点受到攻击不影响其他节点工作，不危害系统安全，扛外部 攻击能力强

信息可信性高：分布式信任模型通过P2P形式的节点间交叉认证，避免内部节点恶 意行为

权力公平性好：与中心化监管相比，无权力层级结构，节点间关系对等，避免权力 滥用与垄断效应

共识与激励机制 P74

PKI 主要应用 P76

数字证书使用

发送方数据加密传输：发送方产生对称密钥；使用对称密钥加密敏感数据；发送方使用接收方的公钽加密对称密钥。

接收方数据加密传输：接受方使用私钥拆开“数字信封”；使用得到的对称密钥解密敏感数据；使用发送方公钥验证数字签名。

加密数据传输：通过数字信封的方式协商对称密钥

HTTPS 协议 本地验证服务器证书，通过 HTTPS 为客户端内置浏览器信任的 CA 颁发的证书

SSL VPN 外出员工与网关，通过证书完成动态的密钥协商

RPKI CA 负责签发源IP 地址和 ASN 的数字证书 P80