蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

公开密钥基础设施

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

区块链基础/区块链密码技术

课程目标

- 了解PKI定义和基本组件
- 了解证书签发与证书吊销

课程目录

PKI定义及功能

PKI定义

- PKI是Public Key Infrastructure的首字母缩写，翻译过来就是公开密钥基础设施。
- PKI是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。
- PKI技术是一种遵循既定标准的密钥管理平台，它的基础是加密技术，核心是证书服务，支持集中自动的密钥管理和密钥分配，能够为所有的网络应用提供加密和数字签名等密码服务及所需要的密钥和证书管理体系。

PKI的功能

- 管理加密密钥和证书的公布，提供密钥管理、证书管理和策略管理等
- 运用数字证书解决数据安全中的私密性、完整性、不可否认性等问题

PKI基本组件

一个典型、完整、有效的PKI应用系统至少应该具有以下部分

数字证书
——包含了用于签名和加密数据的公钥的电子凭证，是PKI的核心元素

认证中心（CA）
——数字证书的申请及签发机关，CA必须具备权威性

证书资料库
——存储已经签发的数字证书和公钥，以及相关证书目录，便于用户获取

证书吊销列表
——在有效期内吊销的证书列表，在线证书状态协议OCSP是获得证书状态的国际协议

密钥备份及恢复
——为避免因用户丢失解密密钥而无法解密合法数据的情况，PKI提供备份与恢复密钥的机制。

03 证书签发

基于证书的公钥分发机制

CA的层次结构

03 证书签发

基于证书的公钥分发机制

CA的层次结构

证书的形成和CA定义

基于证书的公钥分发机制

■ 证书的形成

- 互联网络的用户群决不是几个人互相信任的小集体。
- 从法律角度讲互联网用户群体彼此之间都不能轻易信任，所以公钥加密体系采取了另一个办法，将公钥和公钥的主人名字联系在一起，再请一个大家都信得过的有信誉的公正权威机构确认，并加上这个权威机构的签名。这就形成了证书。

■ 什么是CA?

由于证书上有权威机构的签字，所以大家都认为证书上的内容是可信任的；又由于证书上有主人的名字等身份信息，别人就很容易地知道公钥的主人是谁。

权威机构就是电子签证机关，即CA。

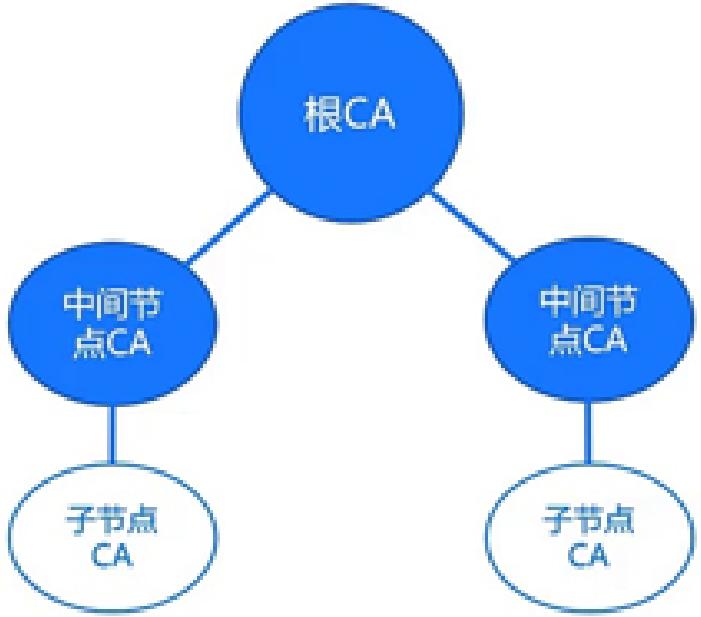
CA的严格层次结构

CA的严格层次结构

其可以表示为一颗倒置的树，根节点代表根CA,它起到信任根或者源头的作用。这个严格层次结构的产生过程是：

1. 根CA为直接在其下的CA创建和签署证书
2. 中间节点代表的CA为其下的子节点CA用户创建和签署证书
3. 倒数第二层的节点代表CA为其下的子节点用户创建和签署证书

在此层次结构中，每个实体都拥有根CA的公钥



证书有效性的管理机制

证书的有效性取决于两个方面因素：

证书有效期：证书的有效期在证书被颁发之日就已经确定了，例如CFCA规定个人证书的有效期是一年（可扩展），企业证书的有效期是三年。已经过了有效期的证书不能通过验证。

证书注销：虽然证书有效期没有过，但是如果发生了特殊情况，例如用户发现证书遗失或私钥失密，用户会向CA/RA提出注销证书的申请，CA/RA经过审核后将实施证书注销。那么，被注销的证书也不能通过验证。

证书吊销管理方案

常用的证书吊销管理方案有两种：

CRL(证书吊销列表)	• CRL是一个具有时间戳的列表，在其中列出了所有已经吊销或挂起的数字证书信息。 • CA管理吊销证书列表，所有客户端应该维护CRLs的缓存。 • 每当CA更新吊销证书列表时，所有的客户端也应该同步更新。
OCSP(在线证书状态协议)	• 用户收到证书验证的请求后，并将请求转发到一个OCSP应答器(服务器)。 • 应答器建立与CA证书库的连接，并查询CA证书库而获得该证书的状态，应答器返回客户机有关证书有效性信息。

总结

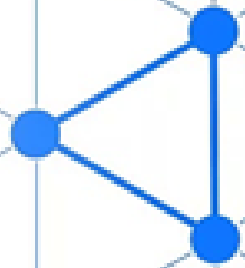
■ PKI

- PKI技术是一种遵循既定标准的密钥管理平台
- PKI的基本组成部分有：数字证书，CA，证书资料库，证书吊销列表和密钥备份及恢复

■ 数字证书

- 用户向CA申请证书，并且CA具有严格的层次机构
- 证书的有效性取决于证书有效期和是否被注销
- 常用的证书吊销管理方案有CRL和OCSP

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN