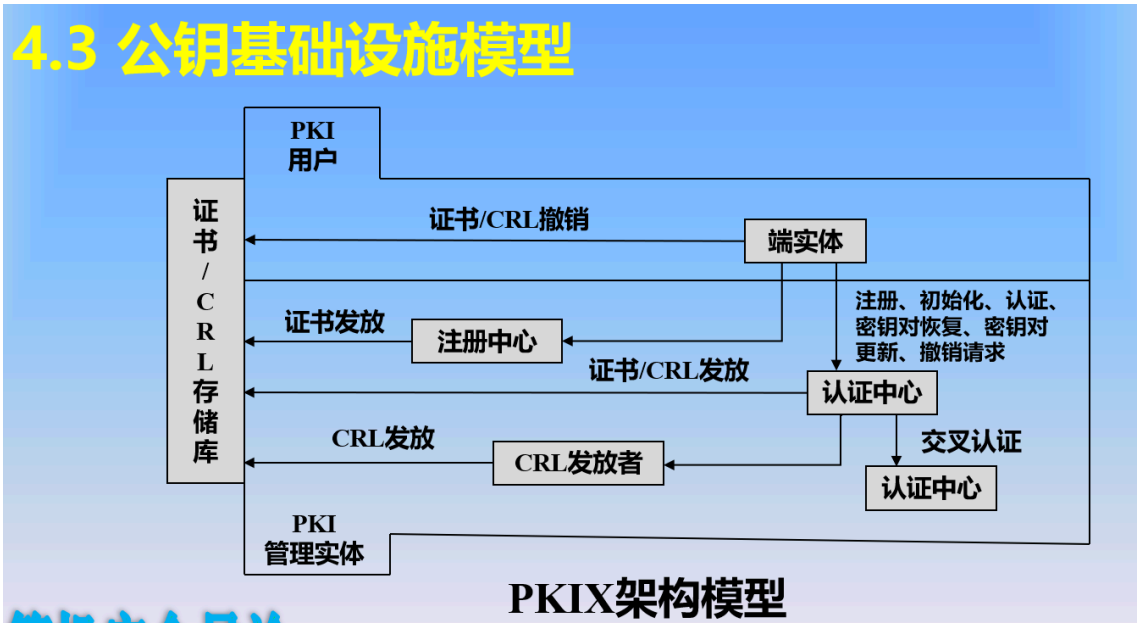
公钥基础设施

- 定义：公钥基础设施（PKI）定义为基于非对称密码体制的用来生成、管理、存储、分配和撤销数字证书的一套硬件、软件、人员、策略和过程。
- 主要要素
  - 端实体：表示终端用户、设备或者其它实体。
  - 认证中心(CA)：证书的发放者。
  - 注册中心（RA）：可选部分，负责端实体的注册过程。
  - 撤销证书列表(CRL)发放者：可选部分，代理CA发布CRL。
  - 存储库：用来存储证书和CRL。
- 模型



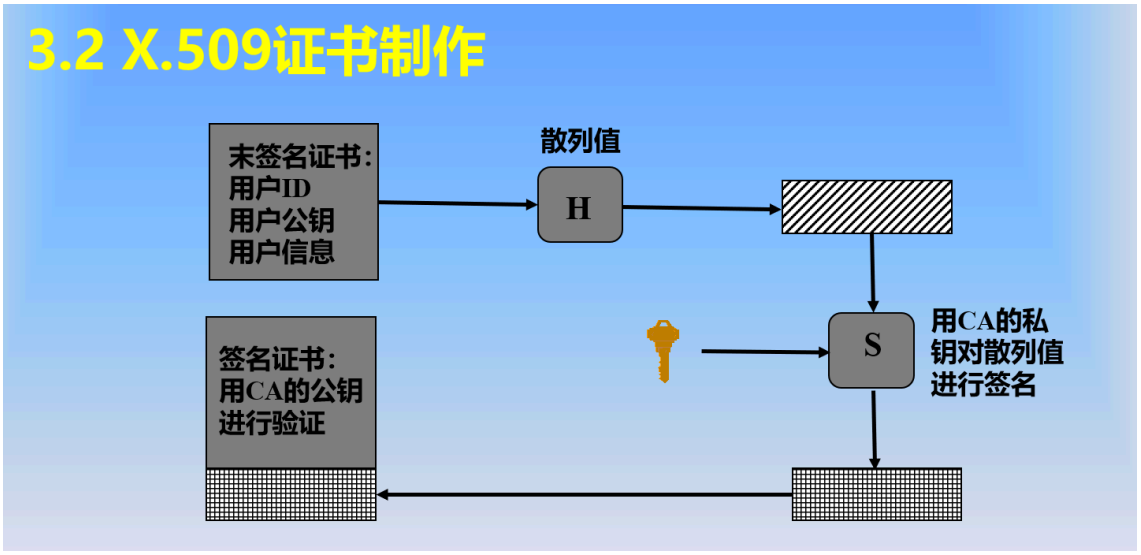
- 功能
  - 注册：让CA知道端实体。
  - 初始化：客户端安装密钥资料。
  - 认证：CA为一个用户的公钥发放一个证书过程。
  - 密钥对恢复：端实体恢复加密/解密密钥对。
  - 密钥对更新：密钥对更新并发放新证书。
  - 撤销申请：撤销已有的公钥证书。
  - 交叉认证：两个CA互相交换用于建立交叉证书信息。

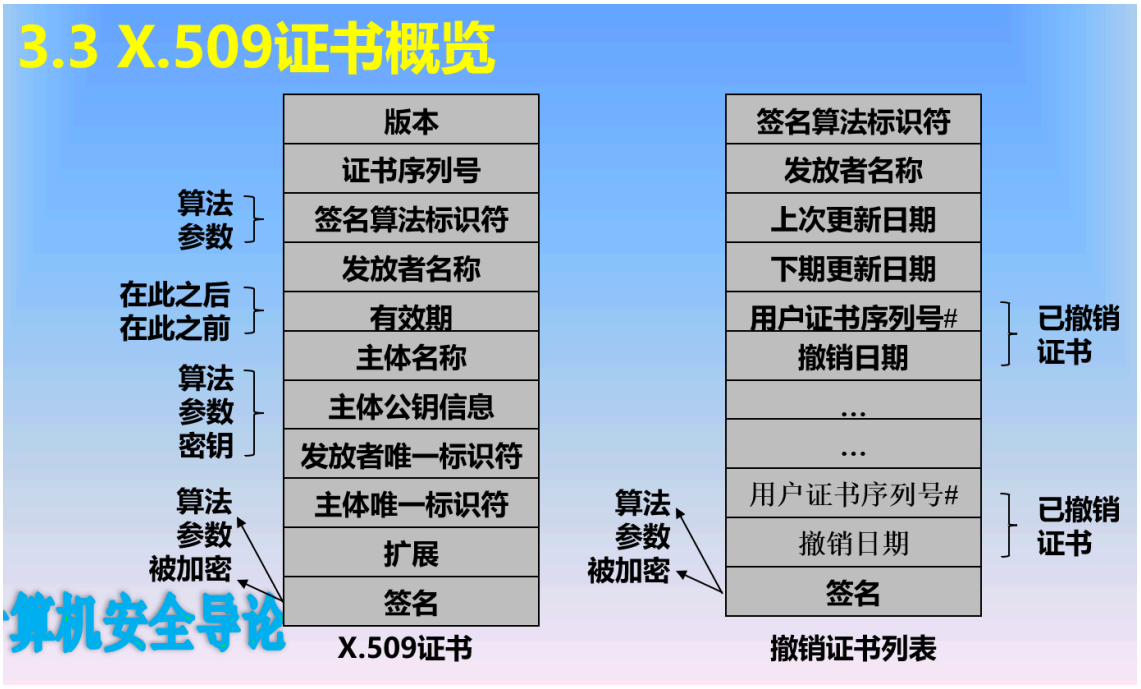
公钥证书

- 定义：由公钥加上公钥所有者的用户ID以及可信的第三方签名的整个数据块组成。
  - 第三方就是用户团体所信任的认证中心(CA)。
  - 用户通过安全渠道把公钥提交给CA获取证书。
  - 发布证书，其它人可以通过CA验证其有效性。

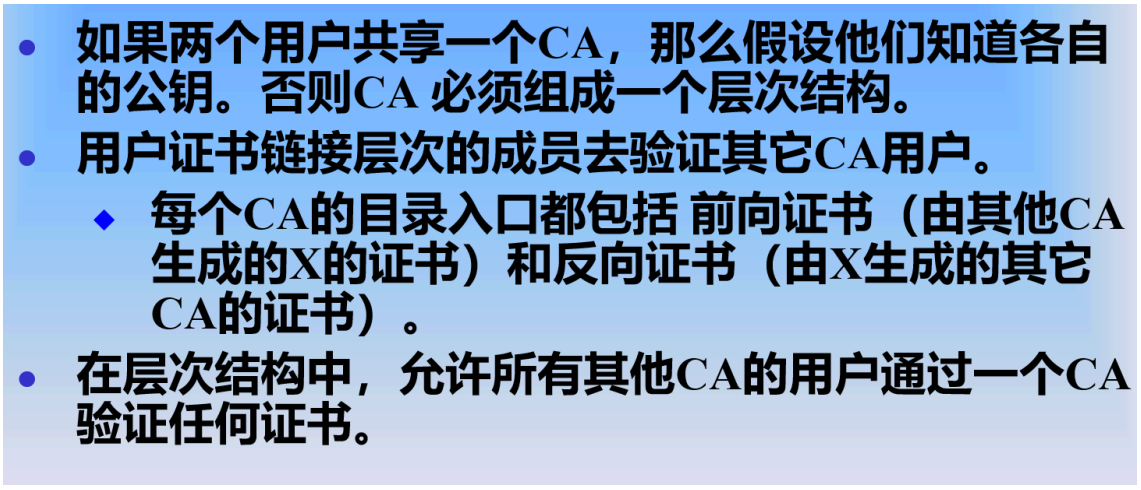
X.509证书（随便看看）

- 定义：X.509定义了一个使用公钥证书存储库向其用户提供认证服务的框架，还定义了另一个基于使用公钥证书的认证协议。

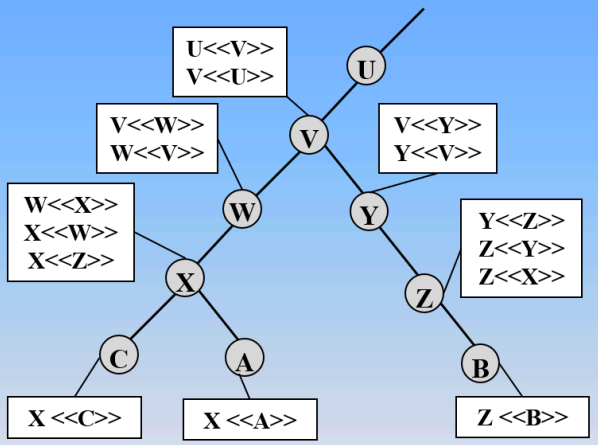




- 获得证书：任何可以访问CA的用户都可以从它获得证书。只有CA可以修改证书。因为不能被伪造，证书可以存放在一个公共字典里。
- CA（认证中心）的层次结构



3.5 CA层次结构



- 证书撤销

- 证书包含一个有效期,可能需要在过期前将其撤销,例如:
  - 用户的私钥被认为已泄露
  - 用户不再被CA信任
  - CA的证书被认为已泄露
- 每个CA都维护被撤销证书的列表(CRL)。
- 用户应该使用CA的CRL检查证书是否被撤销。

- X.509版本3

- 额外的信息应该被包含在证书里，而不是继续在固定的格式上添加新的域
  - email/URL, 策略详细, 使用限制
- 扩展包含:
  - 扩展标识符
  - 危险指标
  - 扩展值

- 扩展包含:
  - 密钥和策略信息:传送关于主体与发放者密钥的附加信息和证书策略指示符。
  - 证书主体和证书发放者属性:支持可选择的名称，发放者可选择的名称，主体目录属性。
  - 认证路径约束：允许在CA发放给CA的证书中包括约束规定。