HTTPS协议详解(三)：PKI 体系

本文大部分内容摘自：http://www.wosign.com/faq/faq2016-0309-03.htm 尊重知识产权，**转载注明Wosign**

----------专栏导航----------

1、RSA身份验证的隐患

身份验证和密钥协商是TLS的基础功能，要求的前提是合法的服务器掌握着对应的私钥。但RSA算法无法确保服务器身份的合法性，因为公钥并不包含服务器的信息，存在安全隐患：

客户端C和服务器S进行通信，中间节点M截获了二者的通信；

节点M自己计算产生一对公钥pub_M和私钥pri_M;

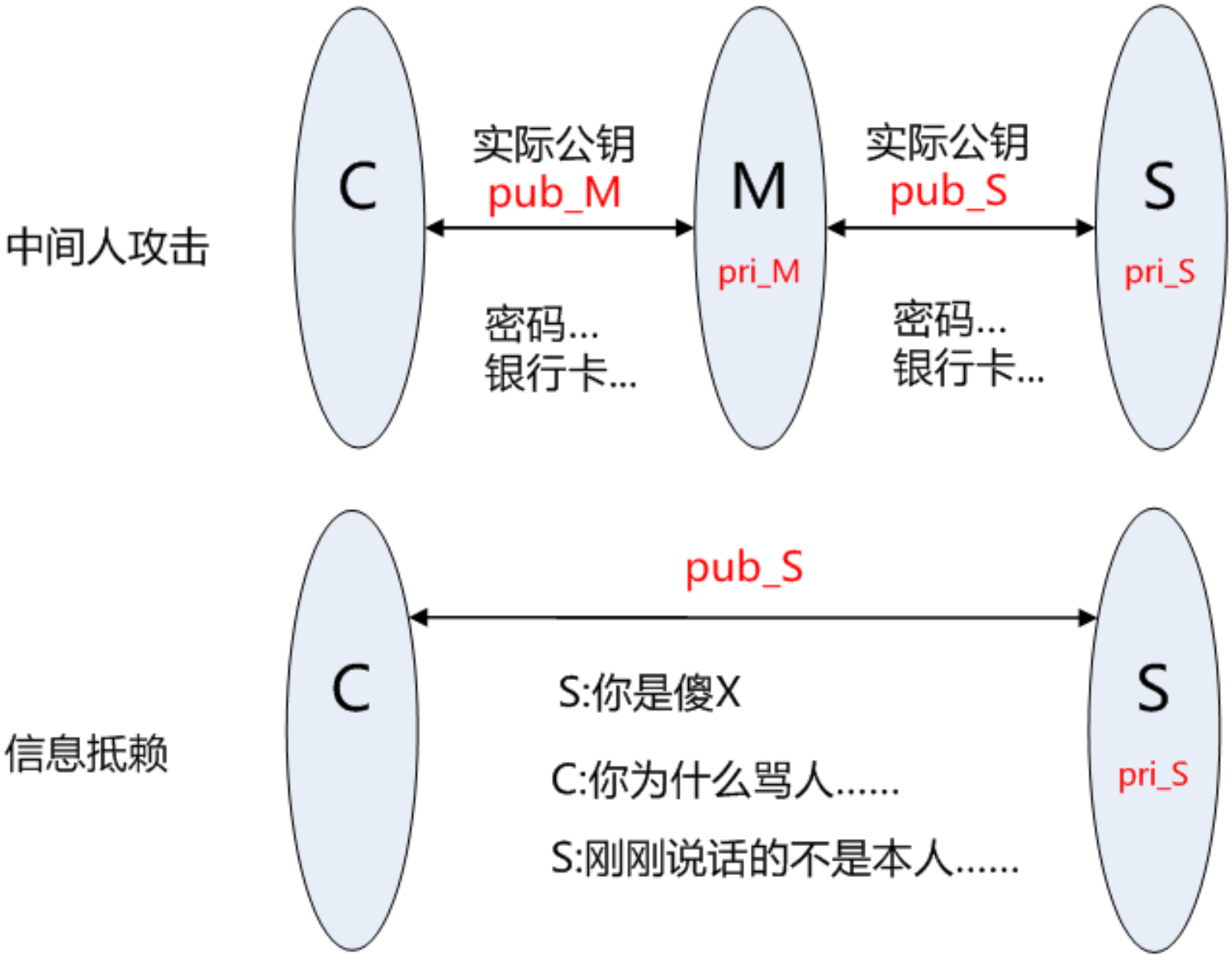
C向S请求公钥时，M把自己的公钥pub_M发给了C;

C使用公钥 pub_M加密的数据能够被M解密，因为M掌握对应的私钥pri_M，而 C无法根据公钥信息判断服务器的身份，从而 C和 M之间建立了"可信"加密连接;

中间节点 M和服务器S之间再建立合法的连接，因此 C和 S之间通信被M完全掌握，M可以进行信息的窃听、篡改等操作。

另外，服务器也可以对自己的发出的信息进行否认，不承认相关信息是自己发出。

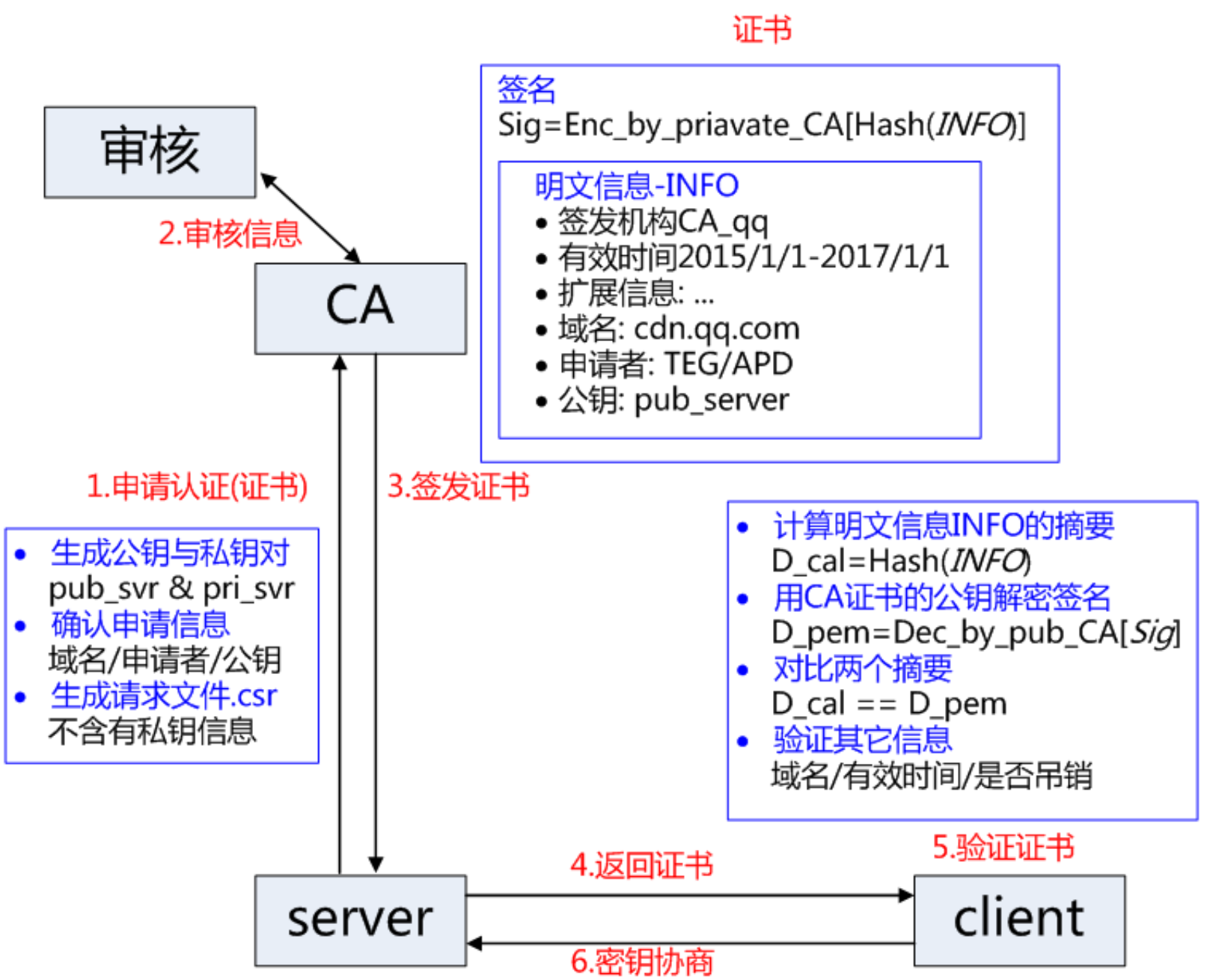
因此该方案下至少存在两类问题：中间人攻击和信息抵赖。



2、身份验证CA和证书

解决上述身份验证问题的关键是确保获取的公钥途径是合法的，能够验证服务器的身份信息，为此需要引入权威的第三方机构CA(如沃通CA)。CA 负责核实公钥的拥有者的信息，并颁发认证"证书"，同时能够为使用者提供证书验证服务，即PKI体系(PKI基础知识)。

基本的原理为，CA负责审核信息，然后对关键信息利用私钥进行"签名"，公开对应的公钥，客户端可以利用公钥验证签名。CA也可以吊销已经签发的证书，基本的方式包括两类 CRL 文件和 OCSP。CA使用具体的流程如下：



a.服务方S向第三方机构CA提交公钥、组织信息、个人信息(域名)等信息并申请认证;

b.CA通过线上、线下等多种手段验证申请者提供信息的真实性，如组织是否存在、企业是否合法，是否拥有域名的所有权等;

c.如信息审核通过，CA会向申请者签发认证文件-证书。

证书包含以下信息：申请者公钥、申请者的组织信息和个人信息、签发机构 CA的信息、有效时间、证书序列号等信息的明文，同时包含一个签名;

签名的产生算法：首先，使用散列函数计算公开的明文信息的信息摘要，然后，采用 CA的私钥对信息摘要进行加密，密文即签名;

d.客户端 C 向服务器 S 发出请求时，S 返回证书文件;

e.客户端 C读取证书中的相关的明文信息，采用相同的散列函数计算得到信息摘要，然后，利用对应 CA的公钥解密签名数据，对比证书的信息摘要，如果一致，则可以确认证书的合法性，即公钥合法;

f.客户端然后验证证书相关的域名信息、有效时间等信息;

g.客户端会内置信任CA的证书信息(包含公钥)，如果CA不被信任，则找不到对应 CA的证书，证书也会被判定非法。

在这个过程注意几点：

a.申请证书不需要提供私钥，确保私钥永远只能服务器掌握；

b.证书的合法性仍然依赖于非对称加密算法，证书主要是增加了服务器信息以及签名；

c.内置 CA 对应的证书称为根证书，颁发者和使用者相同，自己为自己签名，即自签名证书（为什么说"部署自签SSL证书非常不安全"）

d.证书=公钥+申请者与颁发者信息+签名；

★即便有人截取服务器A证书，再发给客户端，想冒充服务器A，也无法实现。因为证书和url的域名是绑定的。

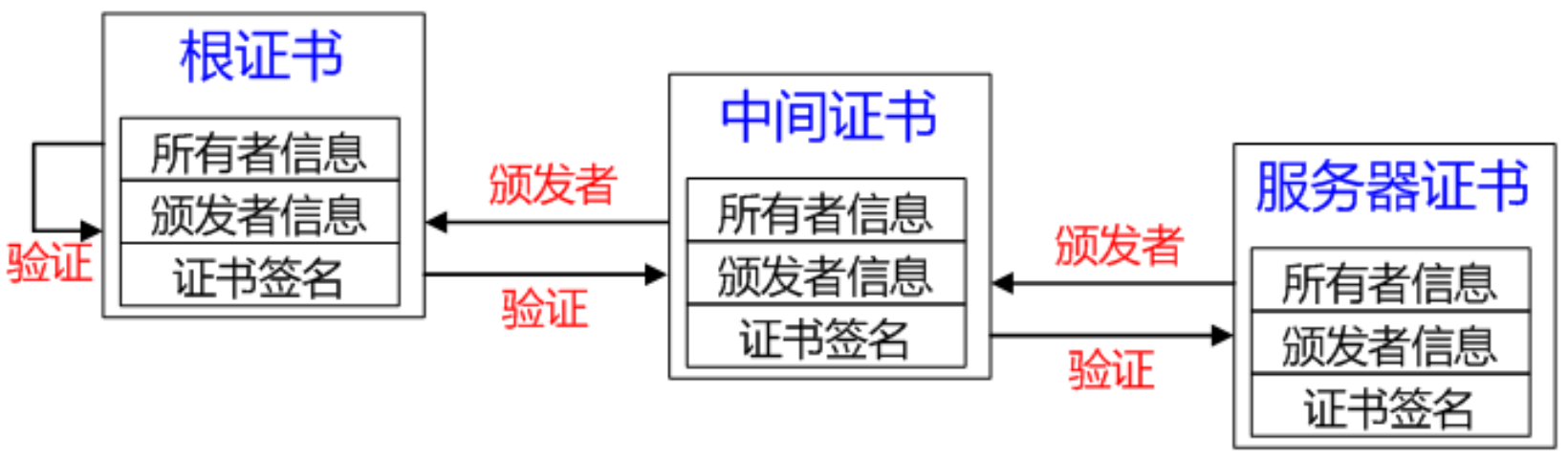
3、证书链

如 CA根证书和服务器证书中间增加一级证书机构，即中间证书，证书的产生和验证原理不变，只是增加一层验证，只要最后能够被任何信任的CA根证书验证合法即可。

a.服务器证书 server.pem 的签发者为中间证书机构 inter，inter 根据证书 inter.pem 验证 server.pem 确实为自己签发的有效证书；

b.中间证书 inter.pem 的签发 CA 为 root，root 根据证书 root.pem 验证 inter.pem 为自己签发的合法证书；

c.客户端内置信任 CA 的 root.pem 证书，因此服务器证书 server.pem 的被信任。



服务器证书、中间证书与根证书在一起组合成一条合法的证书链，证书链的验证是自下而上的信任传递的过程。

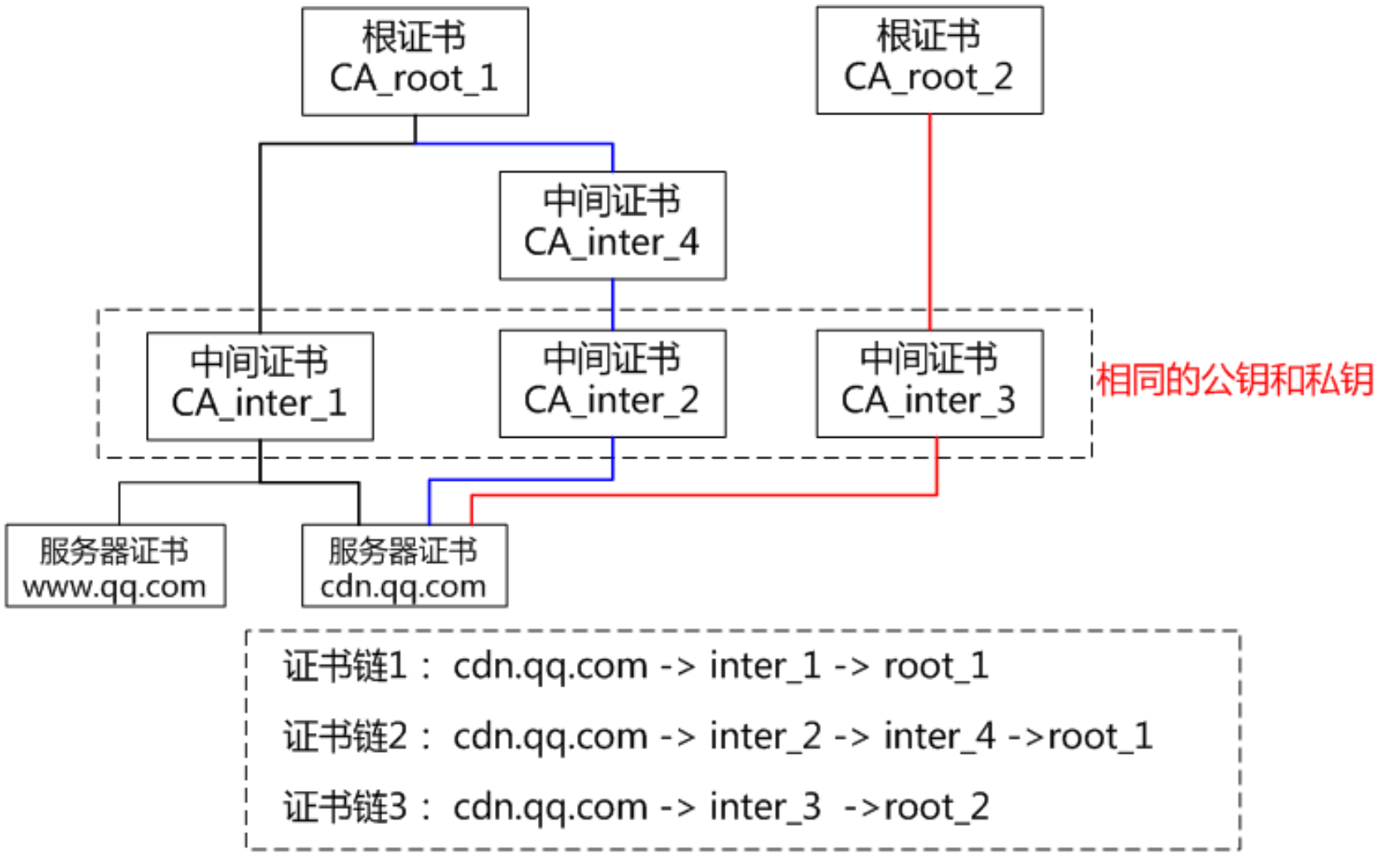
二级证书结构存在的优势：

a.减少根证书结构的管理工作量，可以更高效的进行证书的审核与签发；

b.根证书一般内置在客户端中，私钥一般离线存储，一旦私钥泄露，则吊销过程非常困难，无法及时补救；

c.中间证书结构的私钥泄露，则可以快速在线吊销，并重新为用户签发新的证书;

d.证书链四级以内一般不会对 HTTPS 的性能造成明显影响。



证书链有以下特点：

a.同一本服务器证书可能存在多条合法的证书链。

因为证书的生成和验证基础是公钥和私钥对，如果采用相同的公钥和私钥生成不同的中间证书，针对被签发者而言，该签发机构都是合法的 CA，不同的是中间证书的签发机构不同;

b.不同证书链的层级不一定相同，可能二级、三级或四级证书链。

中间证书的签发机构可能是根证书机构也可能是另一个中间证书机构，所以证书链层级不一定相同。

4、证书吊销

CA 机构能够签发证书，同样也存在机制宣布以往签发的证书无效。证书使用者不合法，CA 需要废弃该证书;或者私钥丢失，使用者申请让证书无效。主要存在两类机制：CRL 与 OCSP。

a.CRL

Certificate Revocation List, 证书吊销列表(什么是证书吊销列表(CRL)?吊销列表起什么作用)，一个单独的文件。该文件包含了 CA 已经吊销的证

书序列号(唯一)与吊销日期，同时该文件包含生效日期并通知下次更新该文件的时间，当然该文件必然包含 CA 私钥的签名以验证文件的合法性。证书中一般会包含一个 URL 地址 CRL Distribution Point，通知使用者去哪里下载对应的 CRL 以校验证书是否吊销。该吊销方式的优点是不需要频繁更新，但是不能及时吊销证书，因为 CRL 更新时间一般是几天，这期间可能已经造成了极大损失。

b.OCSP

Online Certificate Status Protocol, 证书状态在线查询协议，一个实时查询证书是否吊销的方式。请求者发送证书的信息并请求查询，服务器返回正常、吊销或未知中的任何一个状态。证书中一般也会包含一个 OCSP 的 URL 地址，要求查询服务器具有良好的性能。部分 CA 或大部分的自签 CA (根证书)都是未提供 CRL 或 OCSP 地址的，对于吊销证书会是一件非常麻烦的事情。