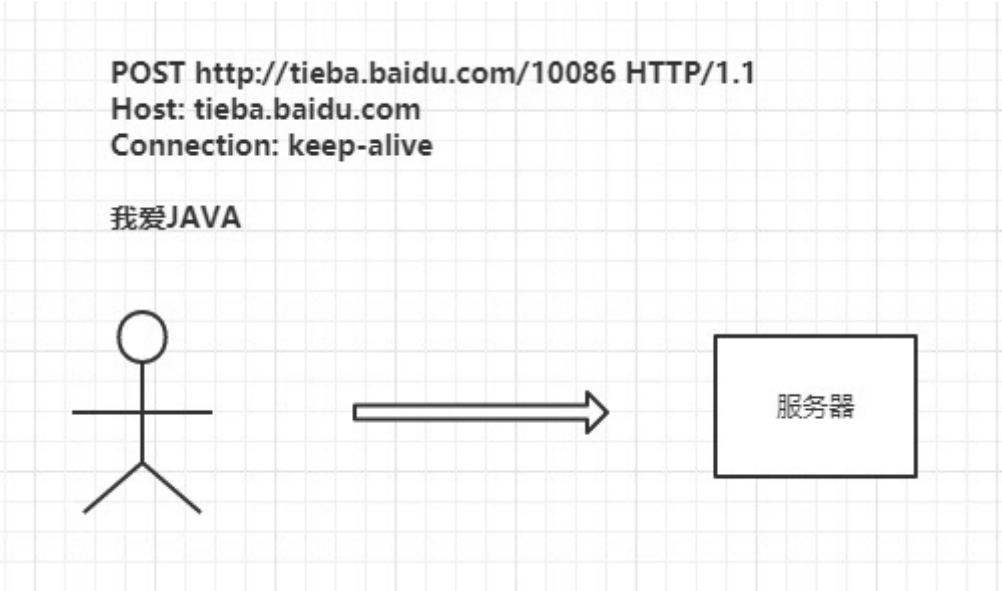
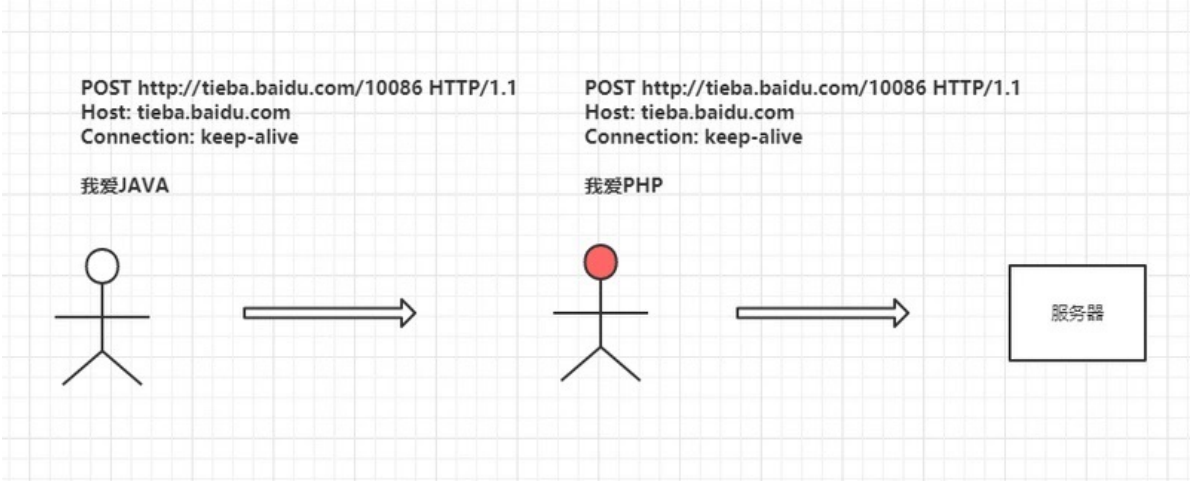
1、HTTP协议

1.1 明文传输中间人攻击

小明在JAVA贴吧发帖，内容为"我爱JAVA":



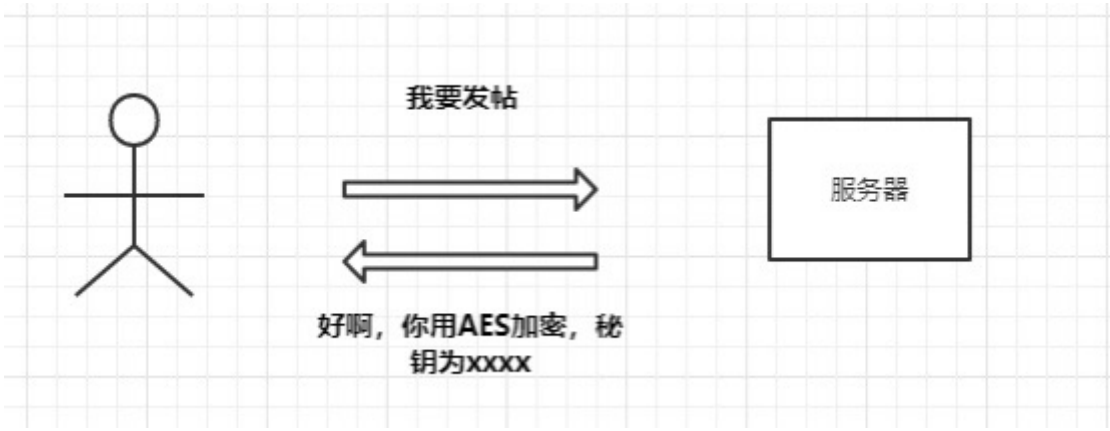
被中间人劫持，内容修改为"我爱PHP":



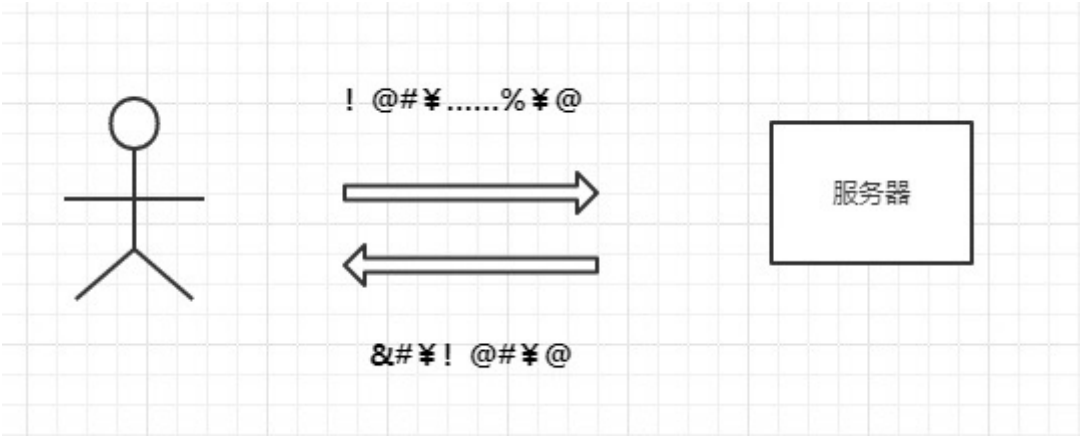
1.2 HTTP加密传输

1.2.1 AES加密传输

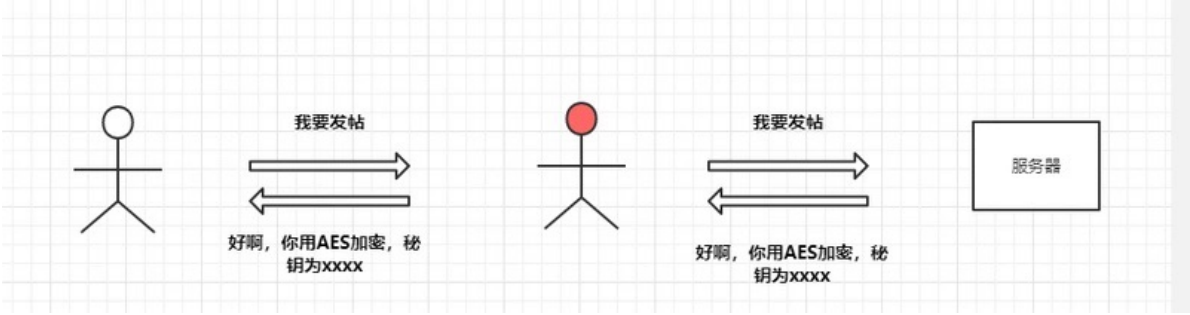
双方约定加密方式:



使用AES加密报文：

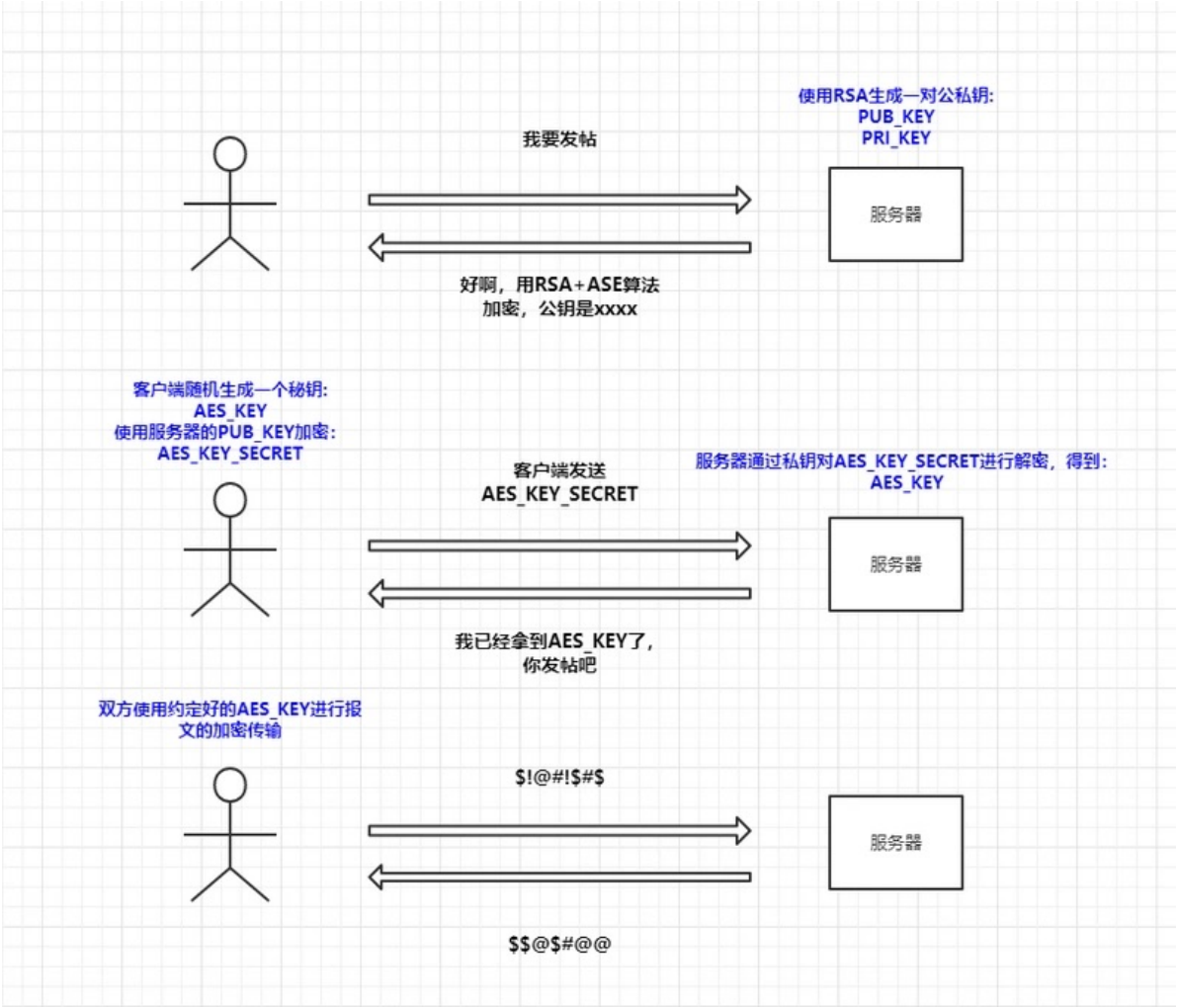


如果第一次通信被窃听，那么秘钥和加密方式会泄露给中间人，中间人仍然可以解密并劫持通信：



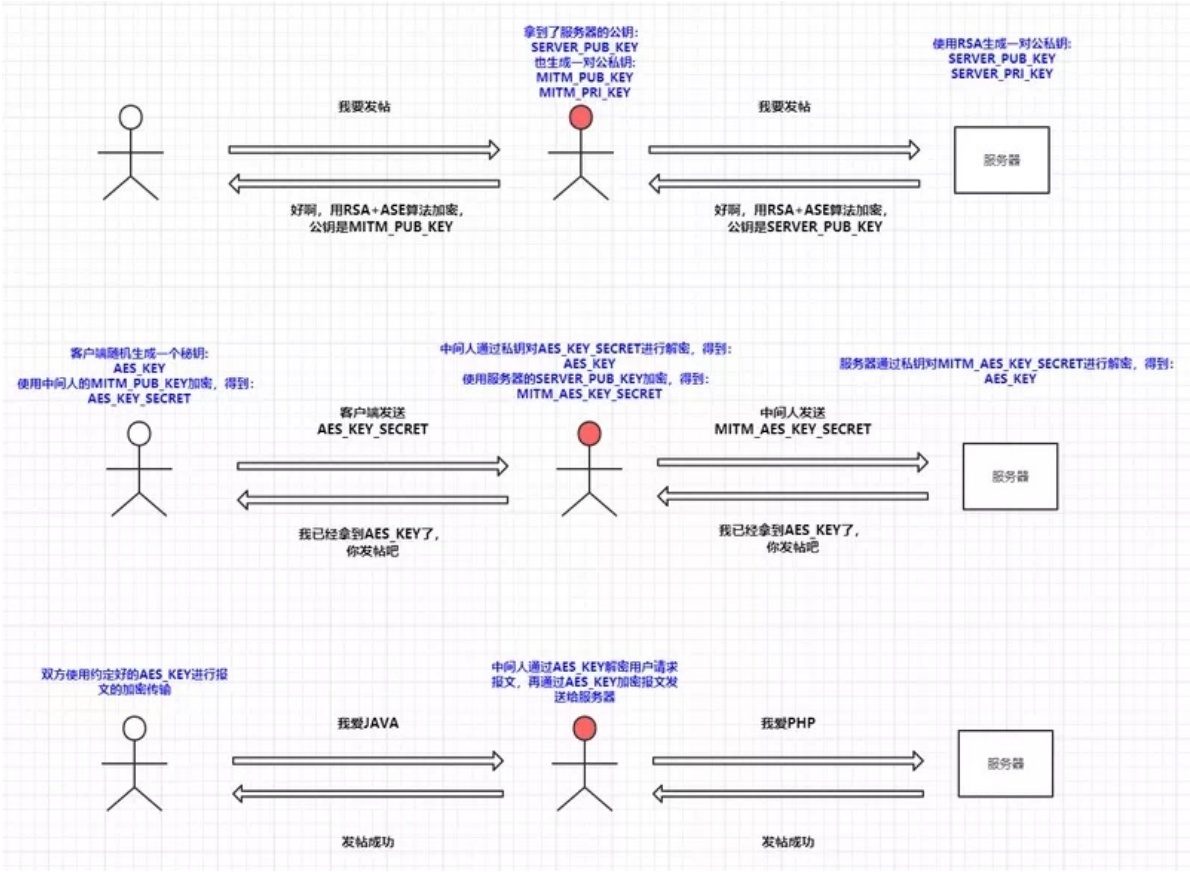
1.2.2 RSA加密传输

为防止秘钥在通信过程中被窃听，服务端生成一对公私钥，并将公钥返回给客户端，客户端本地生成一串AES_KEY，并使用服务端发过来的公钥进行加密得到AES_KEY_SECRET，之后返回给服务端，服务端通过私钥解密得到AES_KEY，最后客户端和服务端通过AES_KEY进行报文的加密通讯：



1.3 加密传输中间人攻击

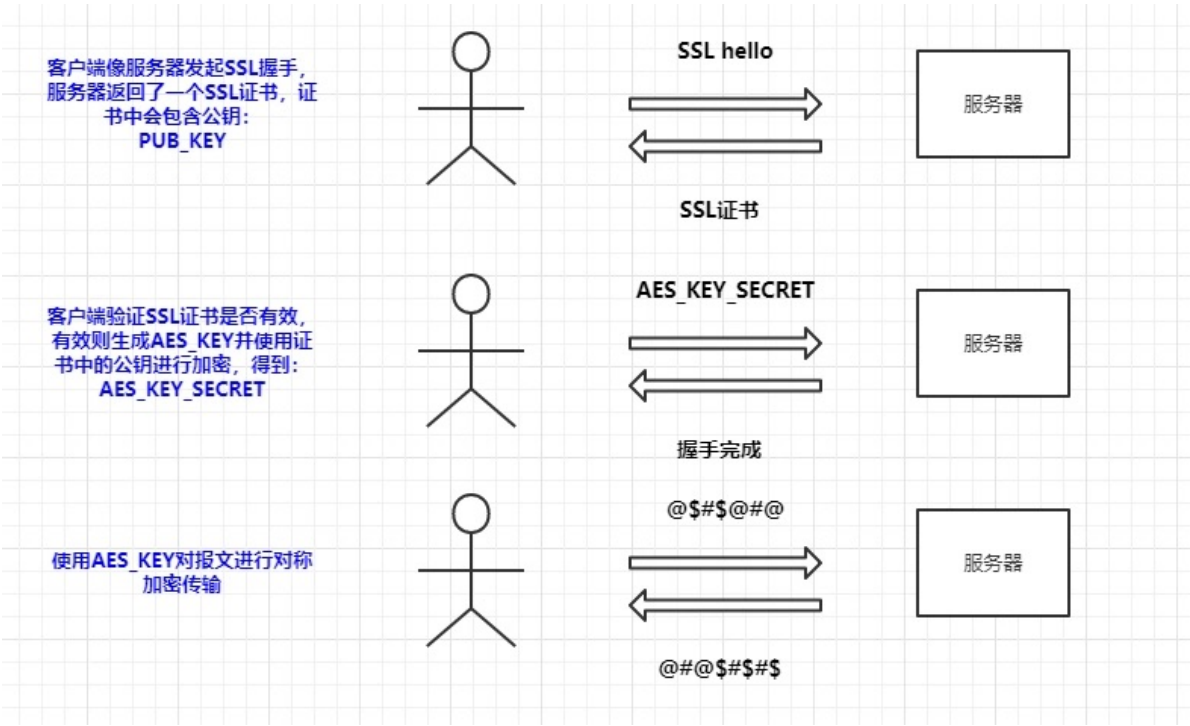
为了破解加密传输，中间人将自己伪装成客户端和服务端的结合体，在用户 -> 中间人的过程中模拟服务器的行为，这样就可以拿到用户请求的明文，在中间人->服务器的过程中模拟客户端的行为，这样可以拿到服务器响应的明文，以此来进行中间人攻击：



2、HTTPS协议

2.1 HTTPS传输原理

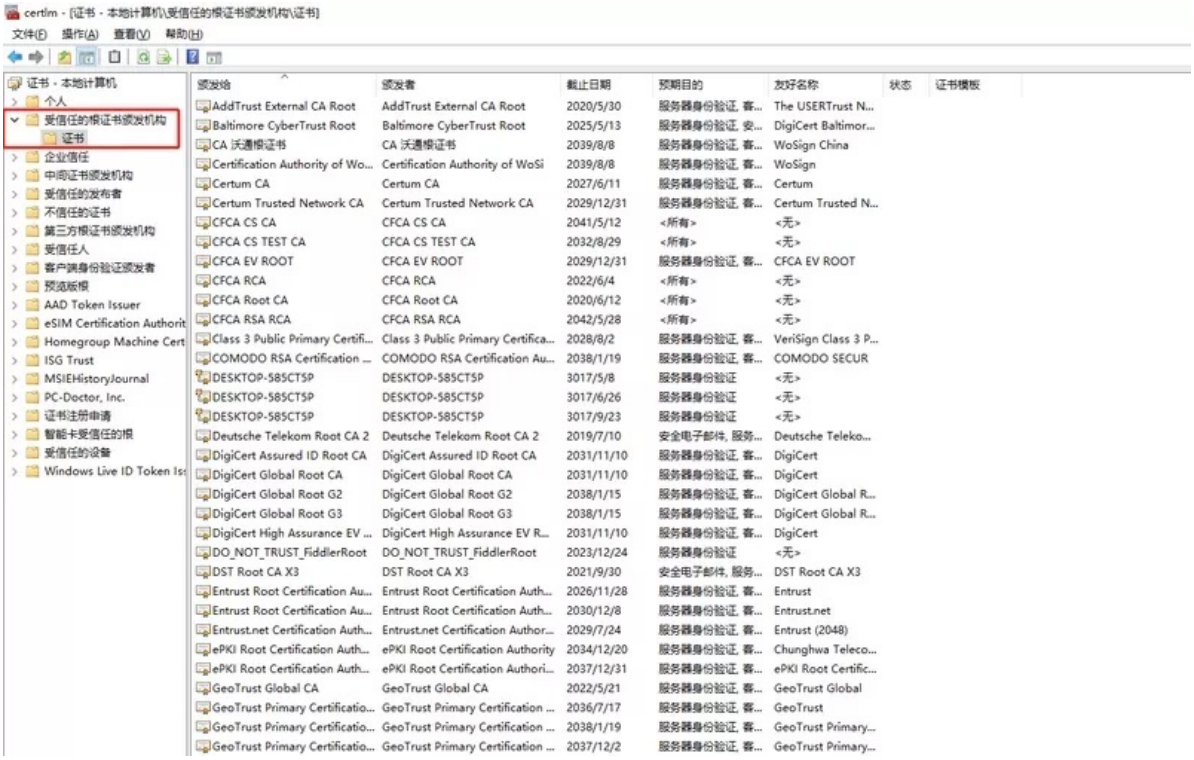
服务端通过SSL证书传递公钥，同时客户端会对SSL证书进行校验：



2.2 CA认证体系

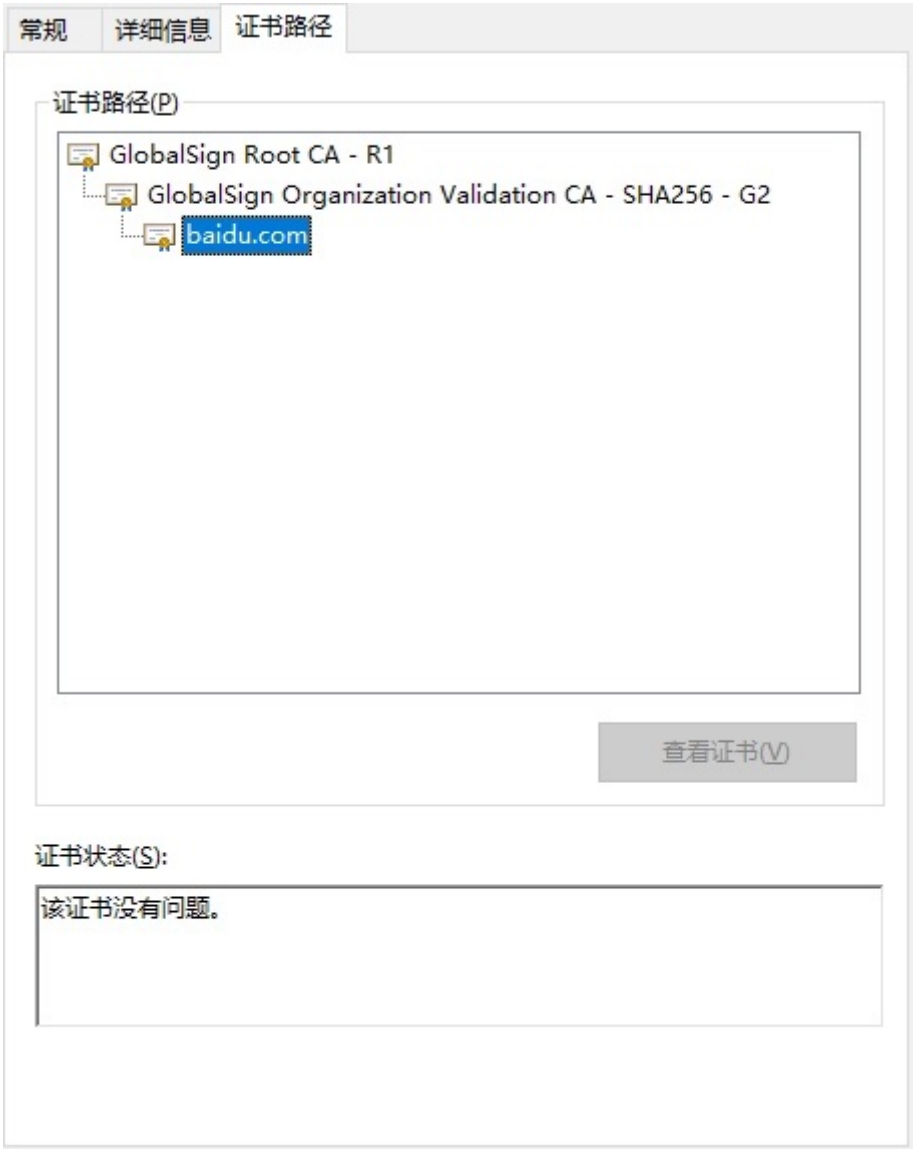
2.2.1 权威认证机构

在CA认证体系中，所有的证书都是权威机构来颁发，而权威机构的CA证书都是内置在操作系统中，这些称之为CA根证书：



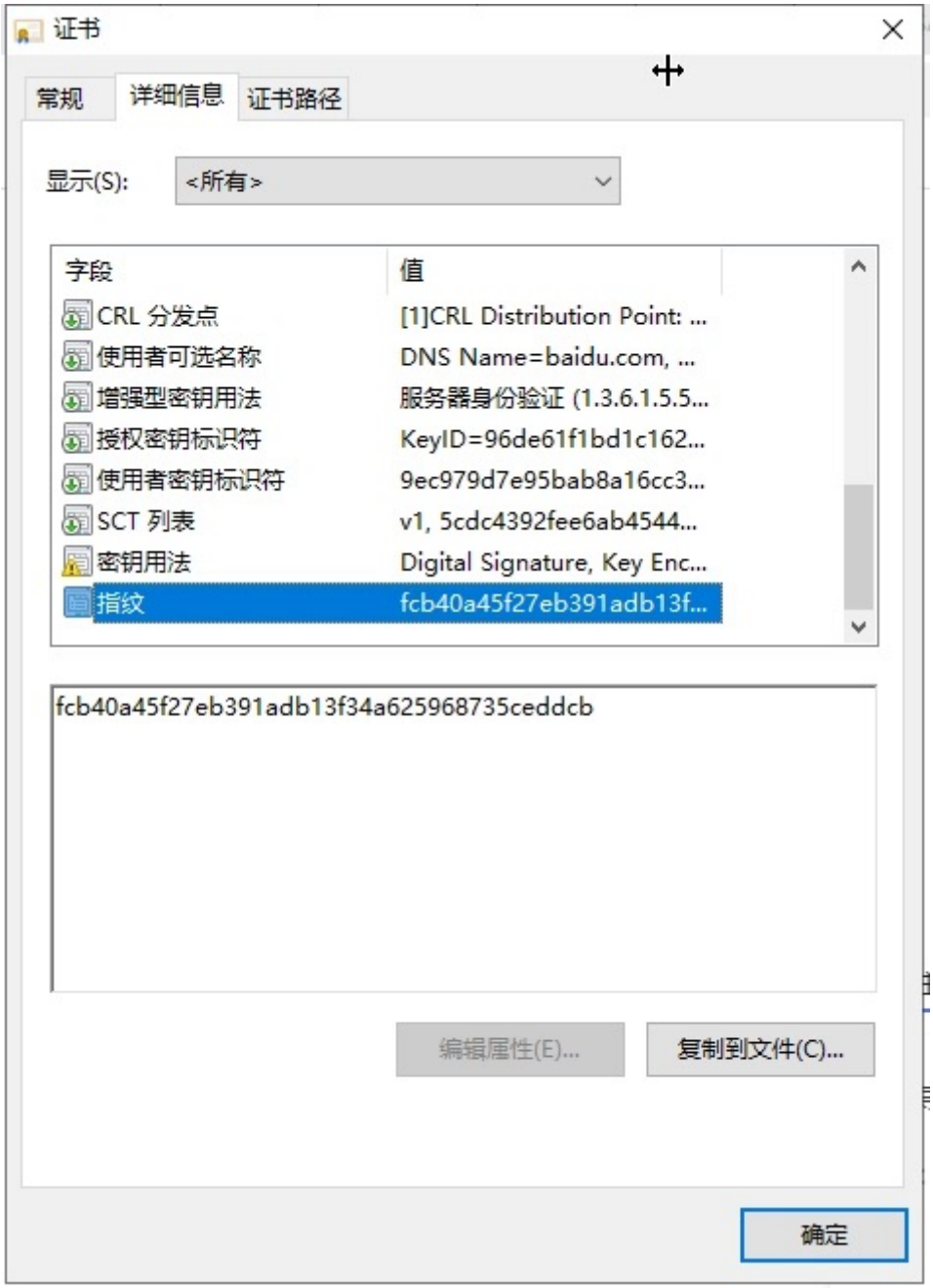
2.2.2 签发证书

服务器如果要使用SSL的话，需要通过权威认证机构来签发CA证书，我们将服务器生成的公钥和站点相关信息发给CA签发机构，再由CA签发机构进行加签得到证书，证书会对生成的证书内容进行签名，并将签名使用CA签发机构的私钥进行加密得到证书指纹，与上级证书生成关系链，下载百度的证书如下：



2.2.3 验证服务器证书

客户端首先通过层级关系找到上级证书，通过上级证书的公钥对服务器的证书指纹进行解密得到签名（sign1），再通过签名算法算出服务器证书的签名（sign2），如果sign1和sign2相同，就说明服务端证书是可以被信任的。


证书
常规
详细信息
证书路径
显示(S):
<所有>
字段
值
CRL 分发点
[1]CRL Distribution Point: ...
使用者可选名称
DNS Name=baidu.com, ...
增强型密钥用法
服务器身份验证 (1.3.6.1.5.5...
授权密钥标识符
KeyID=96de61f1bd1c162...
使用者密钥标识符
9ec979d7e95bab8a16cc3...
SCT 列表
v1, 5cdc4392fee6ab4544...
密钥用法
Digital Signature, Key Enc...
指纹
fcb40a45f27eb391adb13f...
fcb40a45f27eb391adb13f34a625968735ceddcb
编辑属性(E)...
复制到文件(C)...
确定