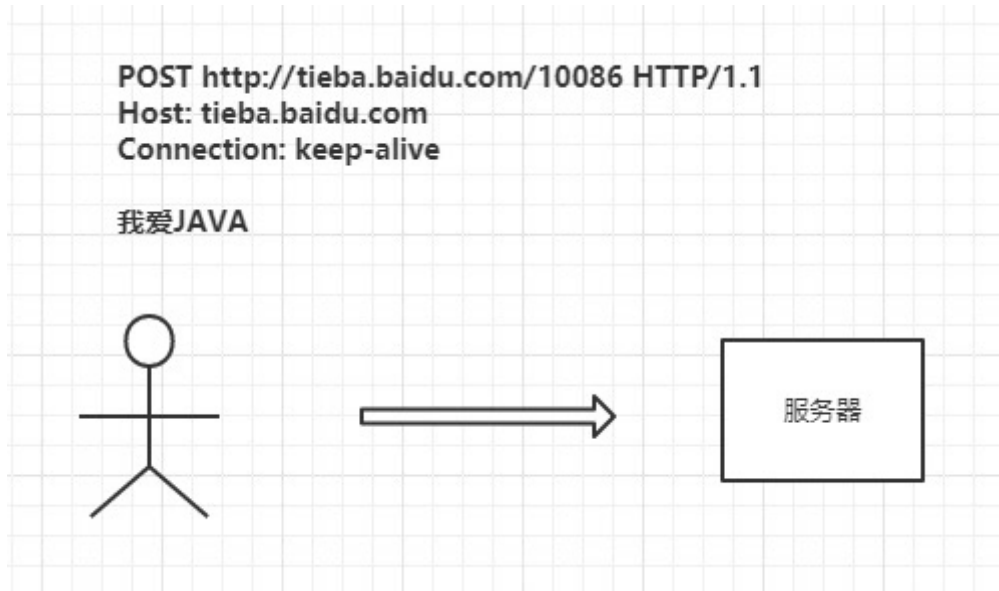


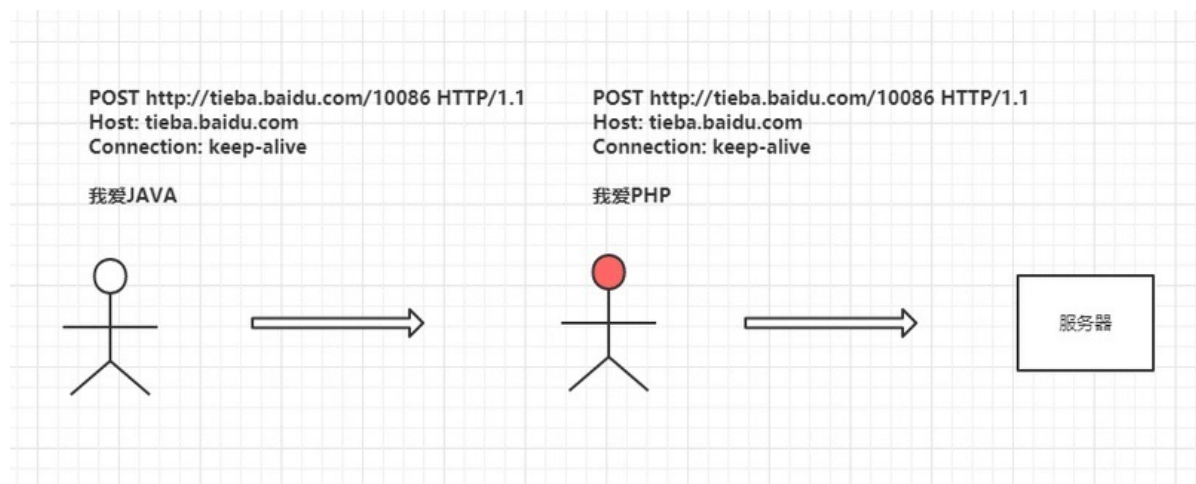
一、HTTP协议

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"：



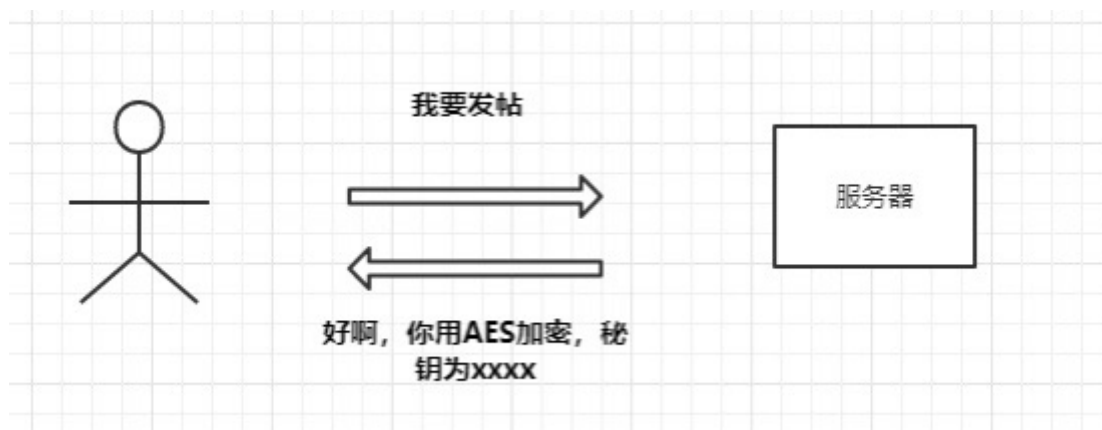
被中间人劫持，内容修改为"我爱PHP"：



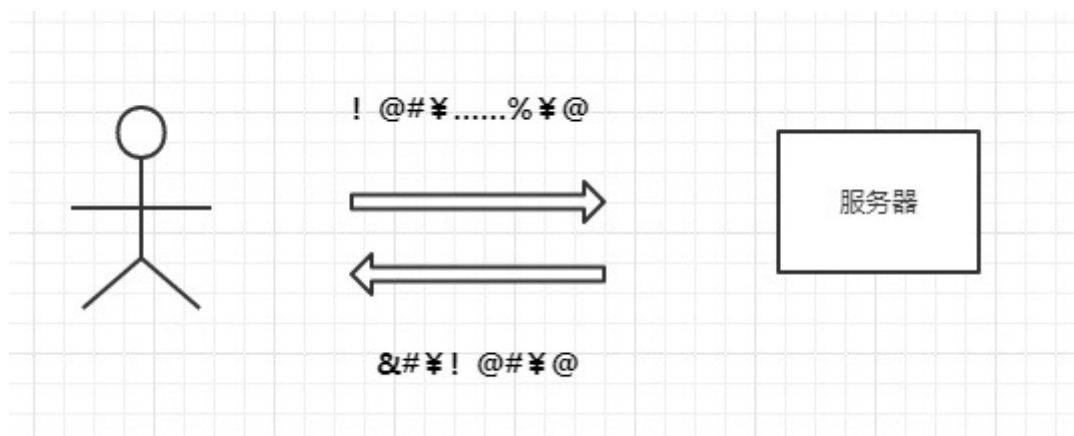
1.2 HTTP加密传输

1.2.1 AES加密传输

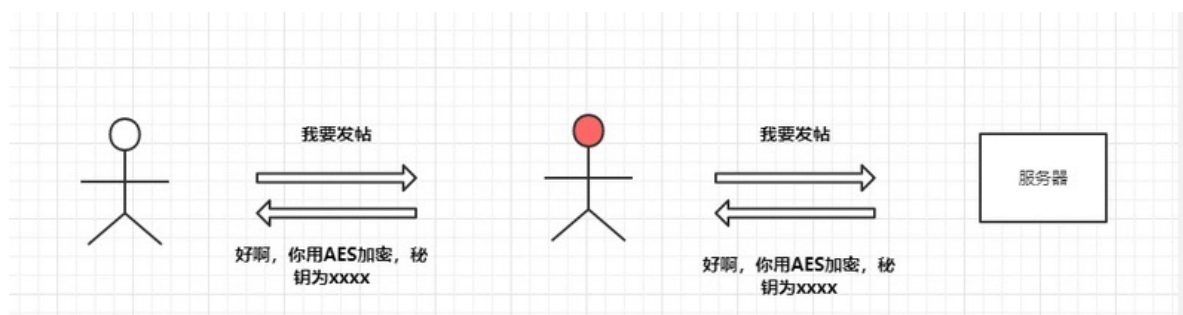
双方约定加密方式：



使用AES加密报文：

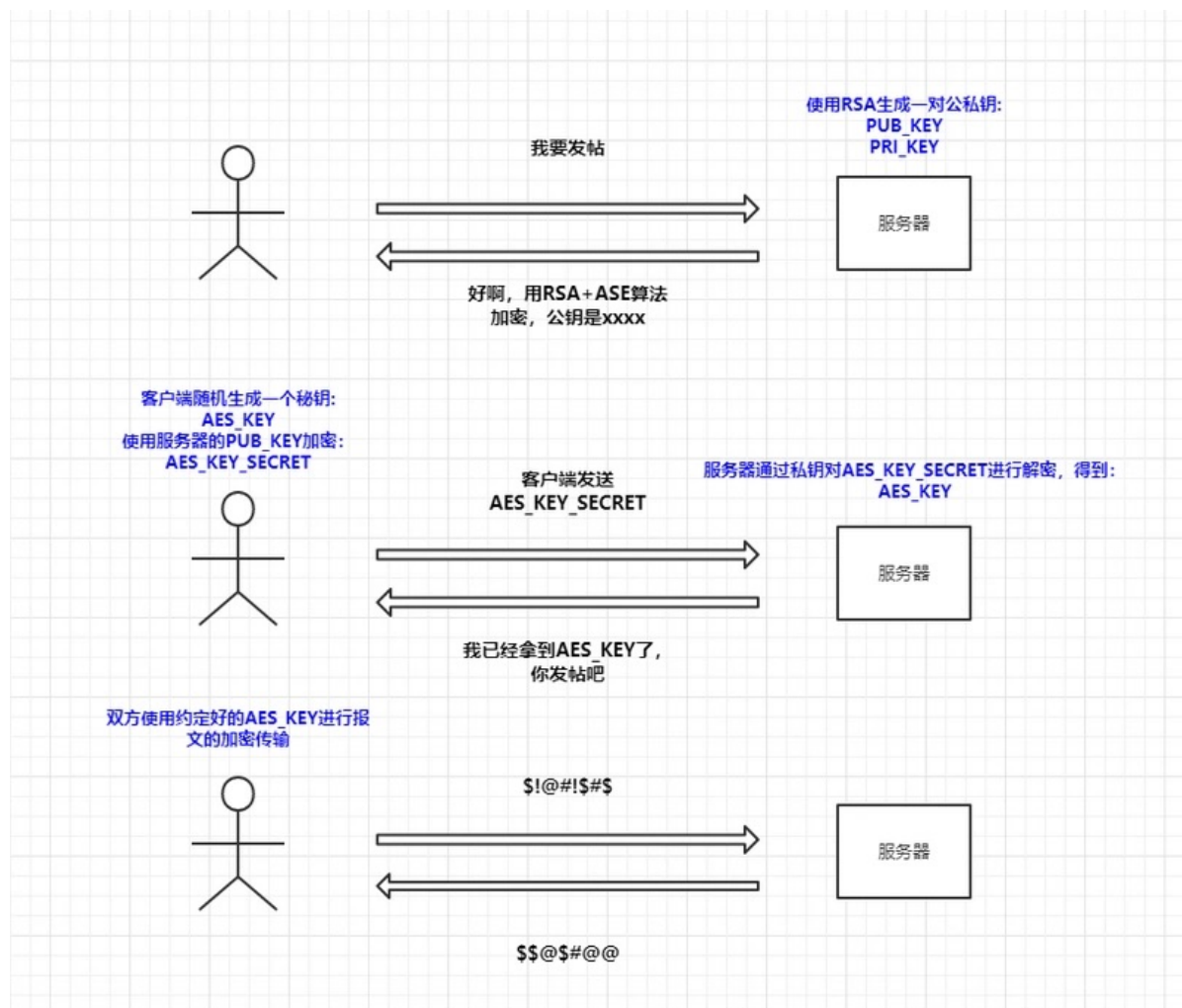


如果第一次通信被窃听，那么密钥和加密方式会泄露给中间人，中间人仍然可以解密并劫持通信：



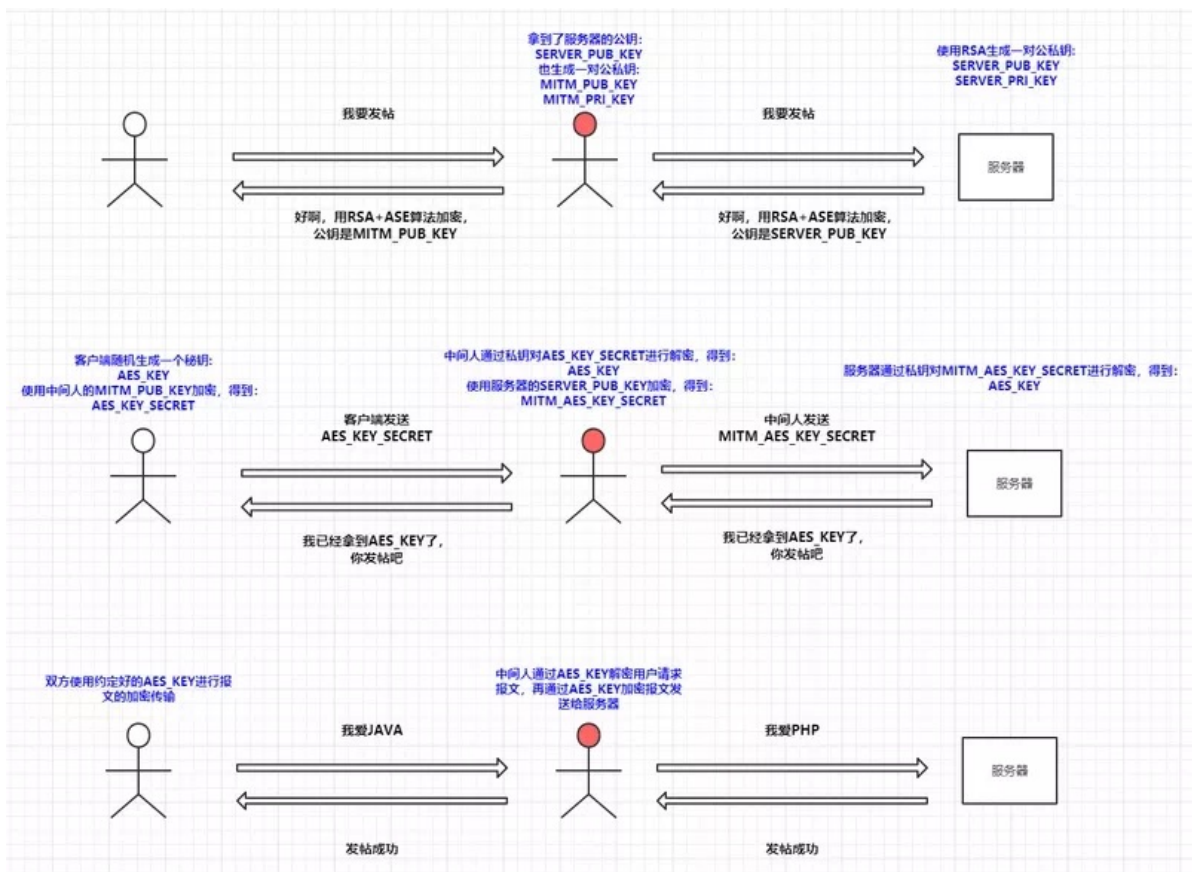
1.2.2 RSA加密传输

为防止密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

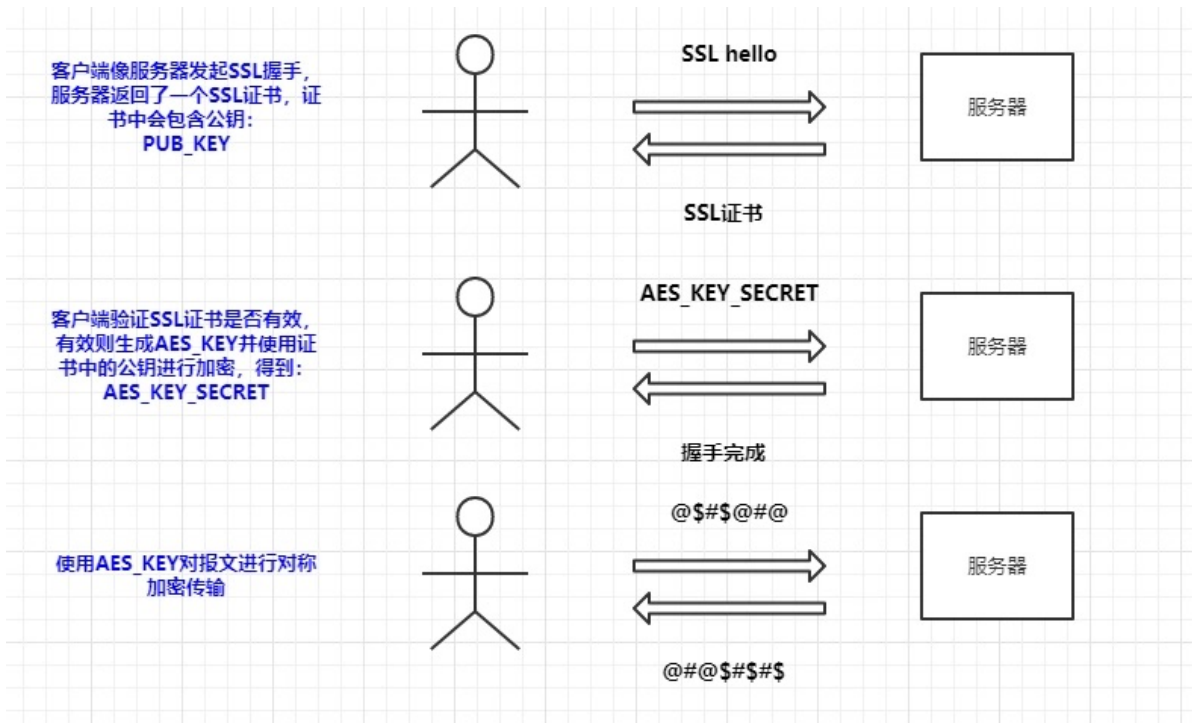
为了破解加密传输，中间人将自己伪装成客户端和服务端的结合体，在用户 -> 中间人的过程中模拟服务器的行为，这样就可以拿到用户请求的明文，在中间人->服务器的过程中模拟客户端的行为，这样可以拿到服务器响应的明文，以此来进行中间人攻击：



二、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：

certmgr.m - [证书 - 本地计算机] 受信任的根证书颁发机构 [证书]

文件(F) 操作(A) 查看(V) 帮助(H)

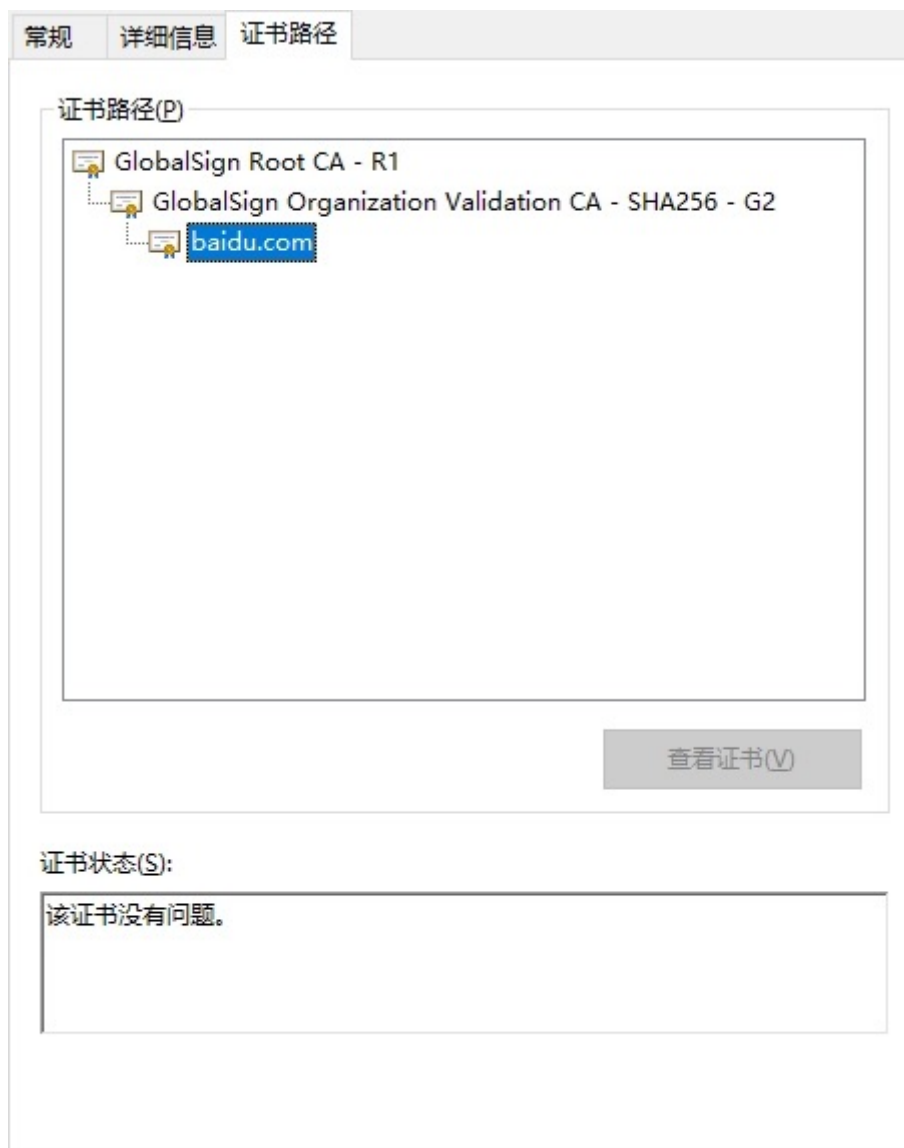
证书 - 本地计算机

受信任的根证书颁发机构

颁发给	颁发者	截止日期	预期目的	友好名称	状态	证书模板
个人						
企业信任						
受信任的根证书颁发机构						
受信任的发布者						
不信任的证书						
第三方信任证书颁发机构						
受信任人						
客户身份验证颁发者						
预览板根						
AAD Token Issuer						
eSIM Certification Authority						
Homegroup Machine Cert						
ISG Trust						
MSIEHistoryJournal						
PC-Doctor, Inc.						
证书注册申请						
智能卡受信任的根						
受信任的设备						
Windows Live ID Token Iss						
AddTrust External CA Root	AddTrust External CA Root	2020/5/30	服务身份验证, 香...	The USERTrust N...		
Baltimore CyberTrust Root	Baltimore CyberTrust Root	2025/5/13	服务身份验证, 安...	DigiCert Baltimor...		
CA 沃通根证书	CA 沃通根证书	2039/8/8	服务身份验证, 香...	WoSign China		
Certification Authority of Wo...	Certification Authority of WoSi	2039/8/8	服务身份验证, 香...	WoSign		
Certum CA	Certum CA	2027/6/11	服务身份验证, 香...	Certum		
Certum Trusted Network CA	Certum Trusted Network CA	2029/12/31	服务身份验证, 香...	Certum Trusted N...		
CFCA CS CA	CFCA CS CA	2041/5/12	<所有>	<无>		
CFCA CS TEST CA	CFCA CS TEST CA	2032/8/29	<所有>	<无>		
CFCA EV ROOT	CFCA EV ROOT	2029/12/31	服务身份验证, 香...	CFCA EV ROOT		
CFCA RCA	CFCA RCA	2022/6/4	<所有>	<无>		
CFCA Root CA	CFCA Root CA	2020/6/12	<所有>	<无>		
CFCA RSA RCA	CFCA RSA RCA	2042/5/28	<所有>	<无>		
Class 3 Public Primary Certifi...	Class 3 Public Primary Certifica...	2028/8/2	服务身份验证, 香...	VeriSign Class 3 P...		
COMODO RSA Certification Au...	COMODO RSA Certification Au...	2038/1/19	服务身份验证, 香...	COMODO SECUR		
DESKTOP-585CTSP	DESKTOP-585CTSP	2017/5/8	服务身份验证	<无>		
DESKTOP-585CTSP	DESKTOP-585CTSP	2017/6/26	服务身份验证	<无>		
DESKTOP-585CTSP	DESKTOP-585CTSP	2017/9/23	服务身份验证	<无>		
Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	2019/7/10	安全电子邮件, 服务...	Deutsche Telekom...		
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	2031/11/10	服务身份验证, 香...	DigiCert		
DigiCert Global Root CA	DigiCert Global Root CA	2031/11/10	服务身份验证, 香...	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	2038/1/15	服务身份验证, 香...	DigiCert Global R...		
DigiCert Global Root G3	DigiCert Global Root G3	2038/1/15	服务身份验证, 香...	DigiCert Global R...		
DigiCert High Assurance EV R...	DigiCert High Assurance EV R...	2031/11/10	服务身份验证, 香...	DigiCert		
DO_NOT_TRUST_FiddlerRoot	DO_NOT_TRUST_FiddlerRoot	2023/12/24	服务身份验证	<无>		
DST Root CA X3	DST Root CA X3	2021/9/30	安全电子邮件, 服务...	DST Root CA X3		
Entrust Root Certification Au...	Entrust Root Certification Auth...	2026/11/28	服务身份验证, 香...	Entrust		
Entrust Root Certification Au...	Entrust Root Certification Auth...	2030/12/8	服务身份验证, 香...	Entrust.net		
Entrust.net Certification Auth...	Entrust.net Certification Author...	2029/7/24	服务身份验证, 香...	Entrust (2048)		
ePKI Root Certification Auth...	ePKI Root Certification Authority	2034/12/20	服务身份验证, 香...	ChungHwa Teleco...		
ePKI Root Certification Auth...	ePKI Root Certification Authori...	2037/12/31	服务身份验证, 香...	ePKI Root Certifi...		
GeoTrust Global CA	GeoTrust Global CA	2022/5/21	服务身份验证, 香...	GeoTrust Global		
GeoTrust Primary Certification...	GeoTrust Primary Certification ...	2036/7/17	服务身份验证, 香...	GeoTrust		
GeoTrust Primary Certification...	GeoTrust Primary Certification ...	2038/1/19	服务身份验证, 香...	GeoTrust Primary...		
GeoTrust Primary Certification...	GeoTrust Primary Certification ...	2037/12/2	服务身份验证, 香...	GeoTrust Primary...		

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。

