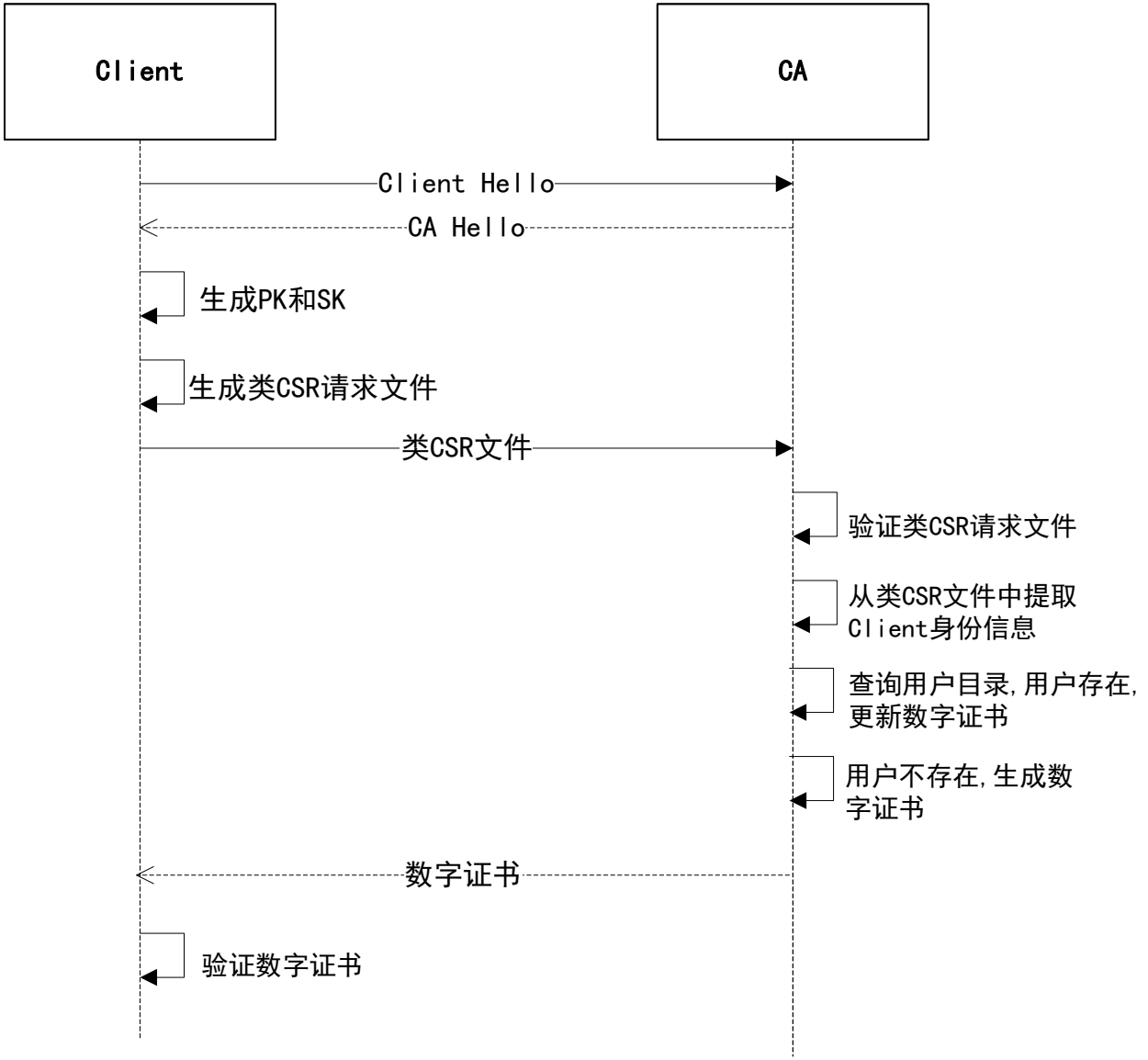
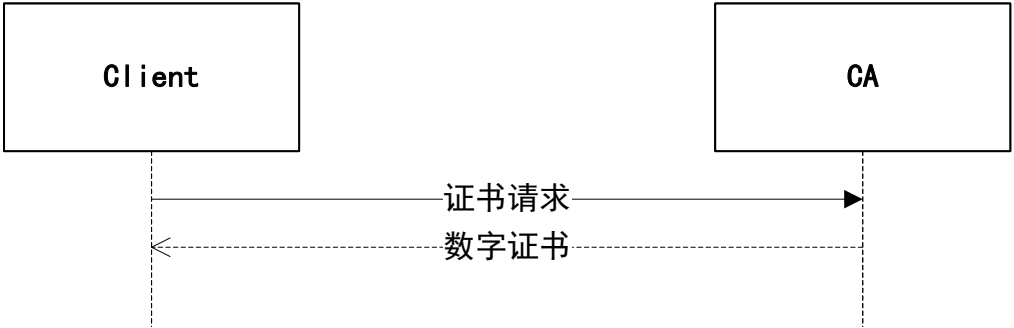
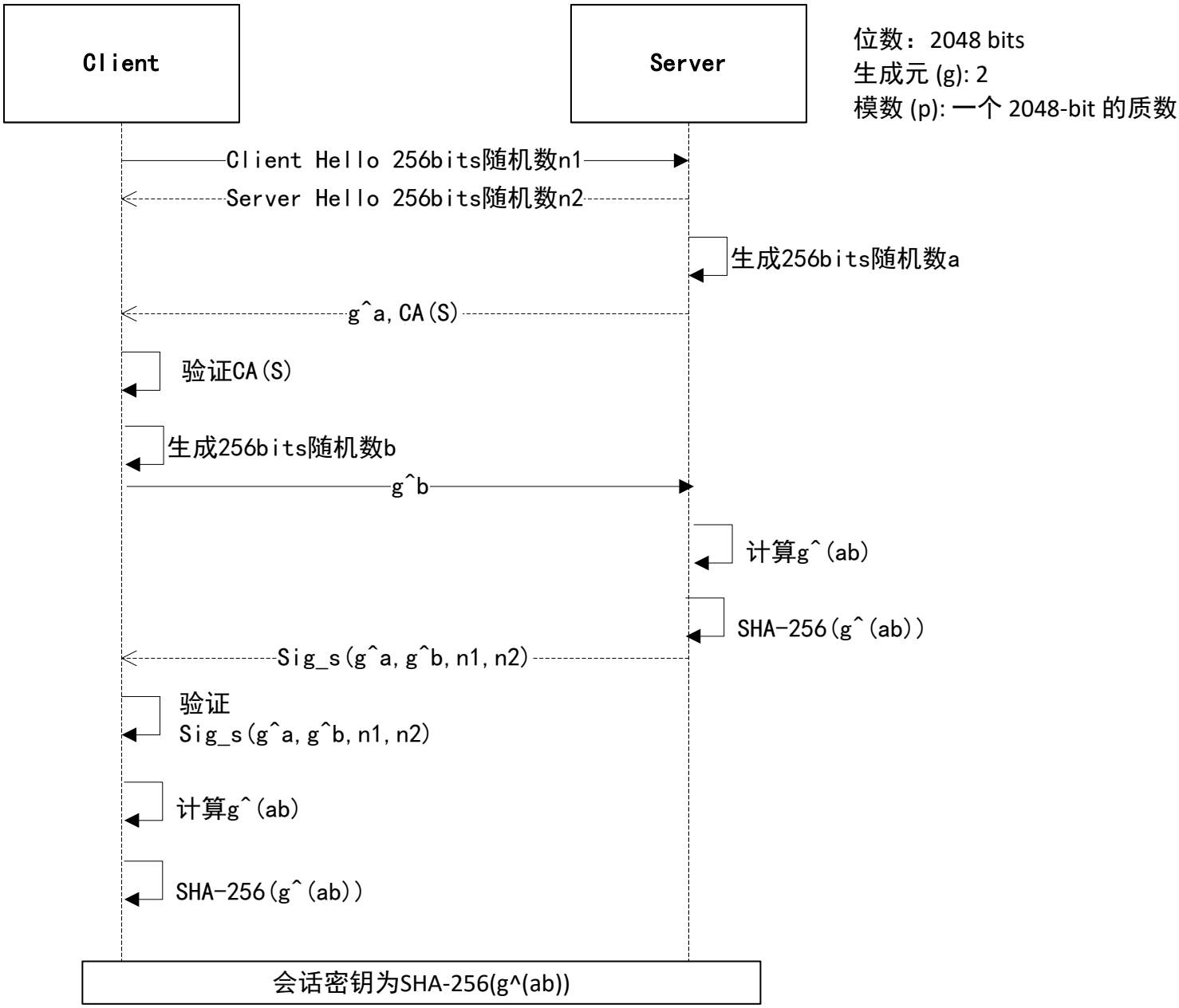
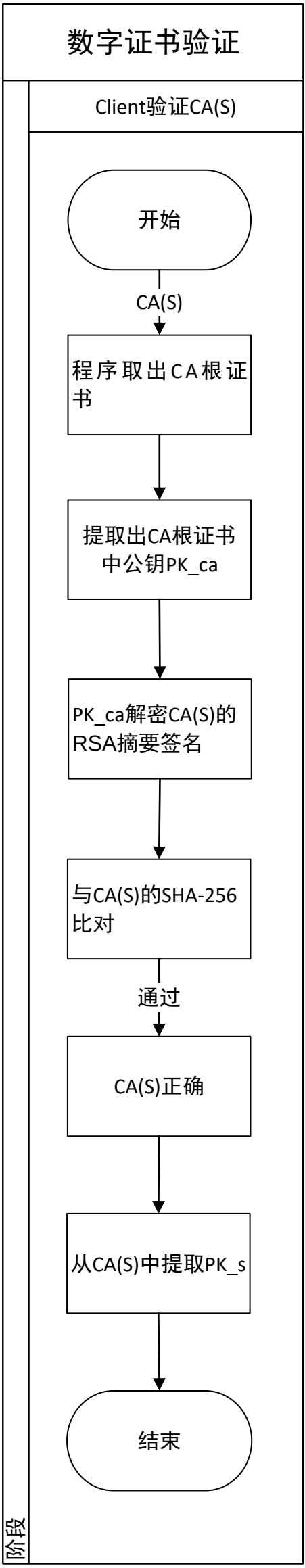

Client
CA
Client Hello
CA Hello
生成PK和SK
生成类CSR请求文件
类CSR文件
验证类CSR请求文件
从类CSR文件中提取
Client身份信息
查询用户目录,用户存在,
更新数字证书
用户不存在,生成数
字证书
数字证书
验证数字证书


Client
CA
证书请求
数字证书

注:默认采用RFC 3526,MODP Group 14:

位数： 2048 bits
生成元 (g): 2
模数 (p): 一个 2048-bit 的质数




数字证书验证
Client验证CA(S)
开始
CA(S)
程序取出CA根证书
提取出CA根证书中公钥PK_ca
PK_ca解密CA(S)的RSA摘要签名
与CA(S)的SHA-256比对
通过
CA(S)正确
从CA(S)中提取PK_s
结束
阶段