# HTTPS

证书

# X.509证书

- 证书
  - 版本号
  - 序列号
  - 签名算法
  - 颁发者
  - 证书有效期
    - 此日期前无效
    - 此日期后无效
  - 主题
  - 主题公钥信息
    - 公钥算法
    - 主题公钥
  - 颁发者唯一身份信息（可选项）
  - 主题唯一身份信息（可选项）
  - 扩展信息（可选项）
    - ...
- 证书签名算法
- 数字签名

openssl x509 -in 证书文件名 -noout -text

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      03:40:28:fe:fd:e8:94:7c:02:a3:49:c7:5c:c2:9e:96
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=CN, O=TrustAsia Technologies, Inc., OU=Domain Validated SSL, CN=TrustAsia TLS RSA CA
    Validity
      Not Before: Aug 20 00:00:00 2018 GMT
      Not After : Oct 19 12:00:00 2019 GMT
    Subject: CN=blog.devmgr.cn
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
          00:98:8a:3a:bb:44: ... ...  5f:89
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Authority Key Identifier:
        keyid:7F:D3:99:F3:A0:47:0E:31:00:56:56:22:8E:B7:CC:9E:DD:CA:01:8A
      X509v3 Subject Key Identifier:
        36:7C:F4:A3:08:88:66:92:88:31:DB:72:A6:AC:F8:00:2F:92:A1:D5
      X509v3 Subject Alternative Name:
        DNS:blog.devmgr.cn
      X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
      X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
      X509v3 Certificate Policies:
        Policy: 2.16.840.1.114412.1.2
          CPS: https://www.digicert.com/CPS
        Policy: 2.23.140.1.2.1
      Authority Information Access:
        OCSP - URI:http://ocsp2.digicert.com
        CA Issuers - URI:http://cacerts.digitalcertvalidation.com/TrustAsiaTLSRSACA.crt
      X509v3 Basic Constraints:
        CA:FALSE
      1.3.6.1.4.1.11129.2.4.2:
        ......w..+\.....F0D. \...;YK.....h.>F!u."..~.N..... h...s{....GSf.....9.....L.0....c
  Signature Algorithm: sha256WithRSAEncryption
    40:5e:a03:ae:67:b73:99:a3: ... ... :c7:2d:86
```

# 证书编码格式

- PEM　Privacy Enhanced Mail

Linux/Unix　Apache NGNIX
openssl x509 -in certificate.pem -text -noout

- DER　Distinguished Encoding Rules

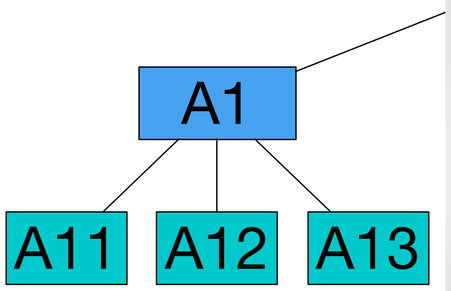
Java Windows
openssl x509 -in certificate.der -inform der -text -noout

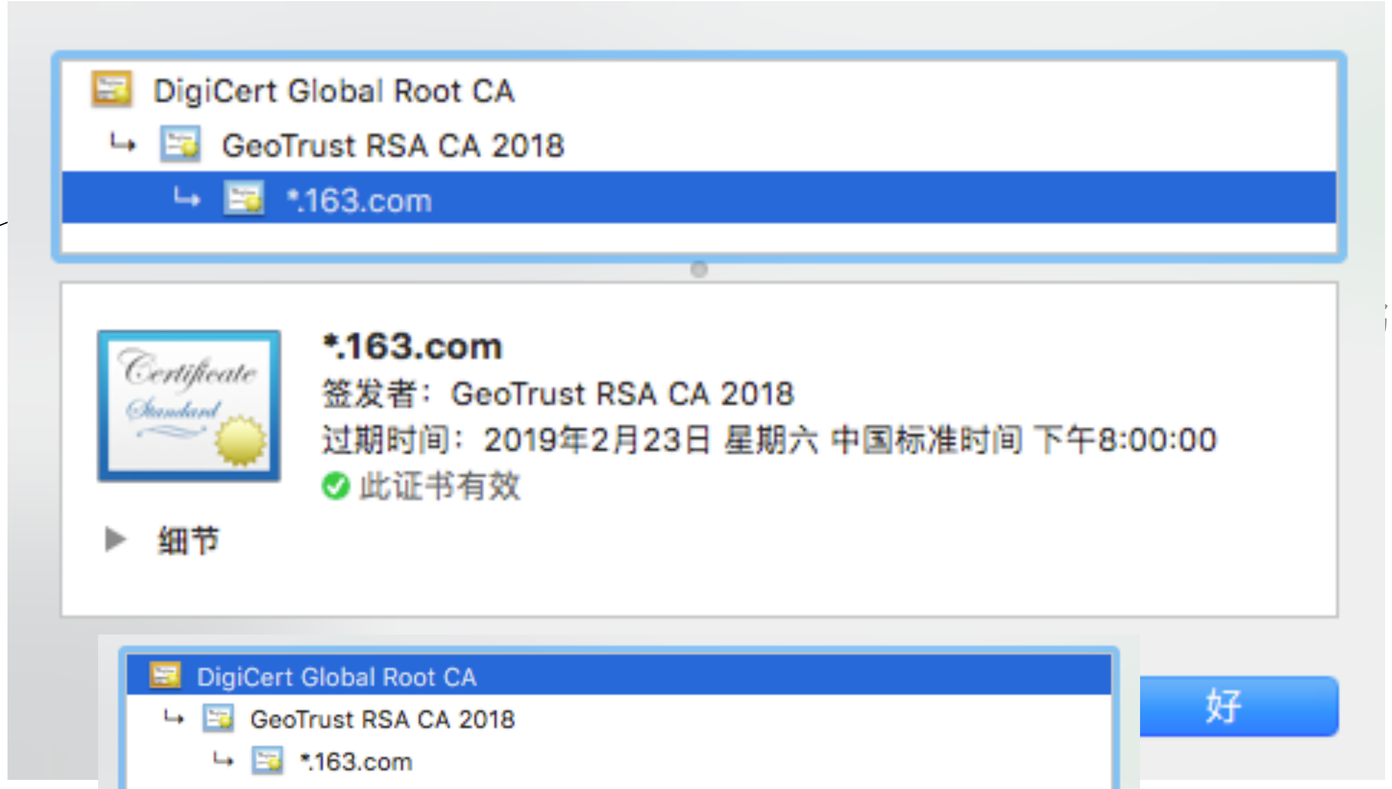
# 证书文件扩展名

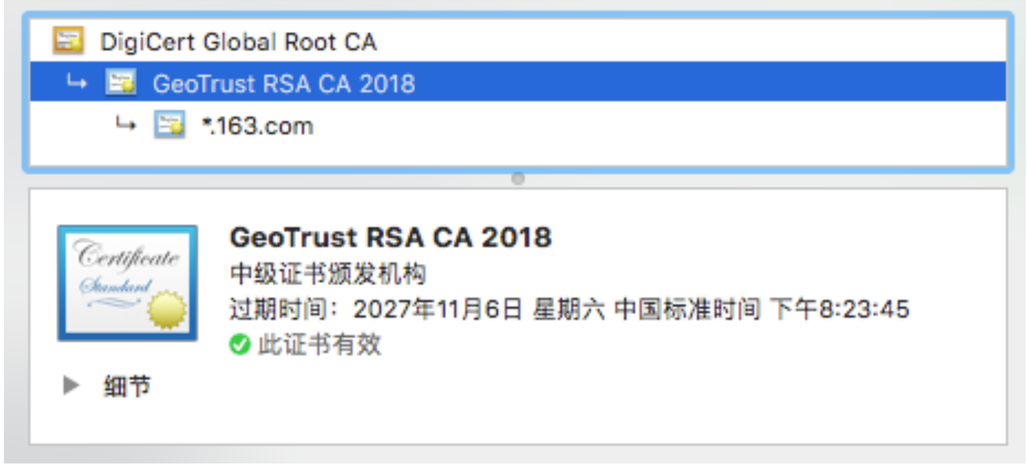
- CRT　证书，Linux/Unix下常用，大多为PEM编码
- CER　证书，windows下常用，大多为DER编码
- CSR　不是证书，Certificate Signing Request，制作证书前的数据，包含信息和公钥
- PFX　包含证书和私钥，IIS使用这种格式，浏览器也可使用
- P12　包含证书和私钥，客户端浏览器证书一般用这种格式
- JKS　Java Key Storage，利用jdk的keytool工具可以把PFX格式转成JKS格式，tomcat中使用这种格式

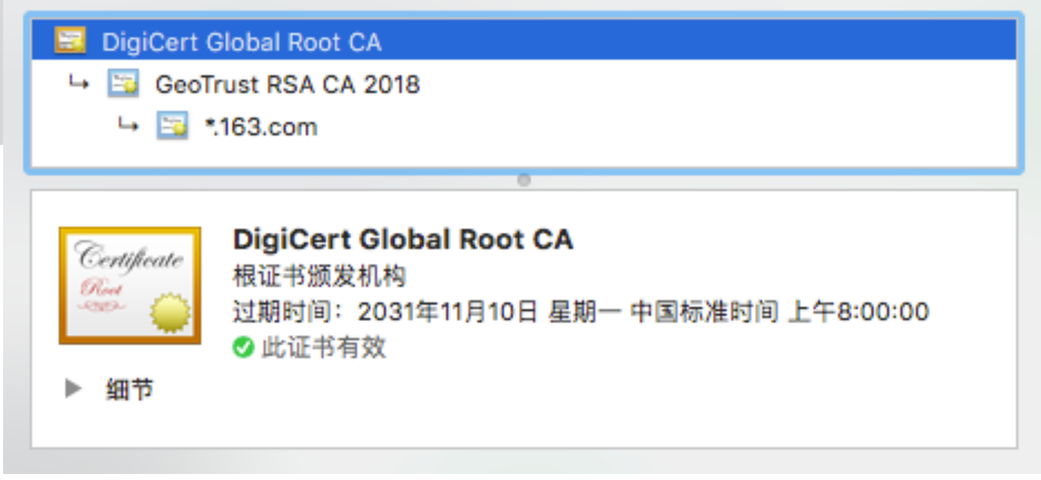
# 证书链

- 朋友的朋友还是朋友

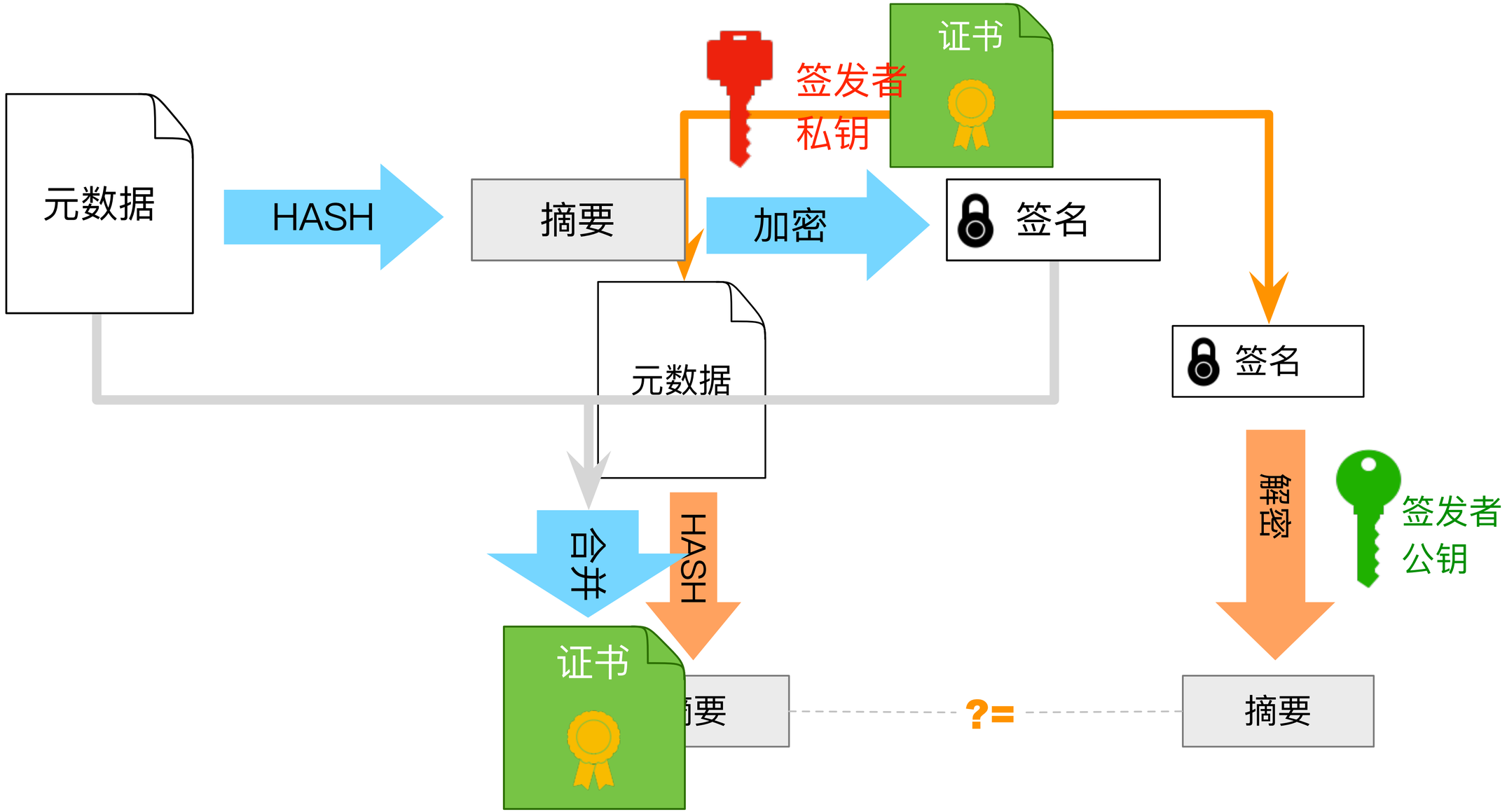


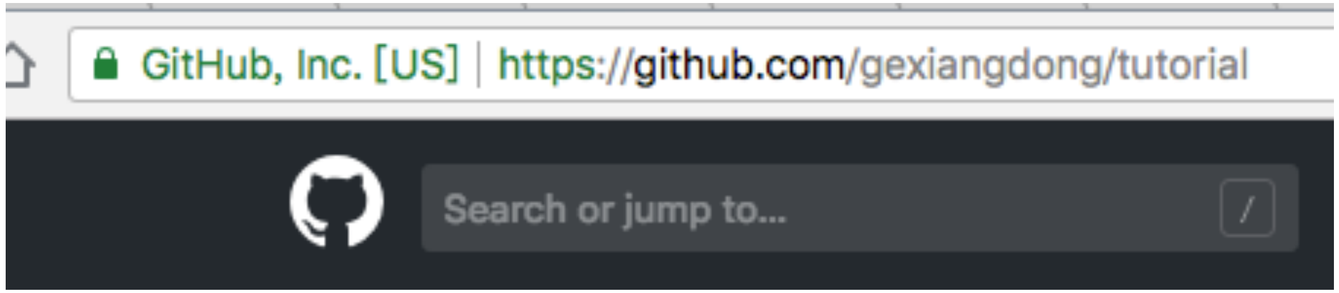



# 证书的签发与验证



# SSL证书的分类

- 域名验证型 DV
- 组织验证型 OV
- 扩展验证型 EV

# 证书的制作

- 自制
  - 工具: OpenSSL
  - 缺点：浏览器不信任，需要每个客户端手工添加自己的CA
  - 可用于小规模，特别是客户端证书
- 购买或申请免费证书