A Brief Introduction to SSL/TLS X.509 Certificates

Wade Cline

January 19, 2018

Outline

Outline

Public/Private Key Cryptography

- *Public* and *Private* key pairs.
- *Share* public keys. *Hide* private keys.
- Simple user: *Many* public keys, *one* private key.
- Public key to *send*, private key to *recieve*.

Network Layers

- Five[1] network *layers*.
  - Application Layer (HTTP, IRC, IMAP, SSH, Git, &c.)
  - **Transport Layer** (TCP/UDP).
  - **Network Layer** (IPv4/IPv6).
  - Link Layer (WiFi, Ethernet).
  - Physical Layer.

[1] No one cares about OSI's 7-layer model.

TLS/SSL

- Naming sucks.
  - SSL (Secure Sockets Layer) – old.
  - TLS (Transport Layer Security) – new.
- Encrypt TCP/IP connections.
- Use *X.509* certificates for *authentication* and *authorization*.
- Various implementations:
  - `openssl`
  - `gnutls`
  - `libressl`

Outline

What does X.509 mean?

- Created in association with X.500 standard.
- Based on ASN.1.
- Defined by the International Telecommunications Union (ITU-T).
- Artists depiction:

Overview

- The *public key* of TLS.
- Called *certificate*.
- *Share* the **certificate**. *Hide* the key.
- Certificate Authorities!
- Confusing terminology!

Certificate Authorities (CAs)

- *Hierarchy* of trust.
- *Root CA* at top, then *Intermediate CAs*.
- Root certificate (Root CA) $\rightarrow$ Intermediate certificate(s)[2] (Intermediate CA(s)) $\rightarrow$ Leaf[3] Certificate[4] (You)
- Path is a certificate *chain of trust*.

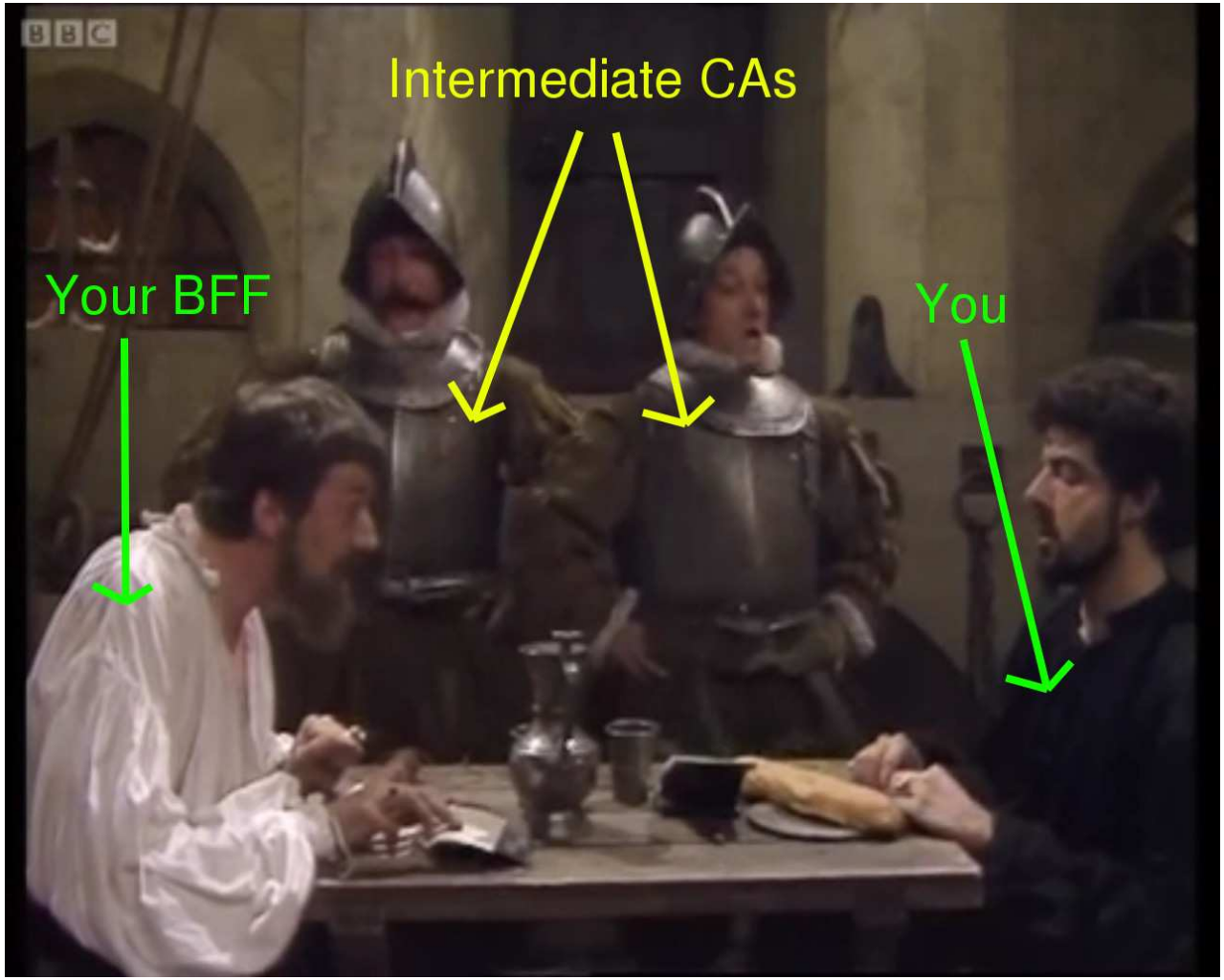
[2] Zero or more.

[3] Do these even have a formal name?

[4] Or just use the root certificate as a leaf certificate. That's cool, too.

Artist's Depiction

Artist's Depiction pt2



Terminology

- Issuer & Subject.
  - Subject *recieves* certificate from issuer.
  - Subject usually *you*.
  - **Bloated** fields consist of **beaurcratic crap**:
    - Country Name ← One world, man.
    - State or Provience Name ← Cascadia, obvs.
    - Locality Name ← wtf?
    - Organization Name ← "A Dude".
    - Organization Unit Name ← W.T.F.?
    - **Common Name** ← Only sane field (usually your FQDN).
    - E-mail Address ← For spambots.
  - CAs *may* omit fields.
- Client and Server certificates.
  - Client certificates rare, often not used on home browsers.

About

- PKI (Public Key Infrastructure).
- Manages certificates.
- Many PKIs.
- Usually browser's implementation.

Viewing

- `/usr/share/ca-certificates/`
- Subdirectories possible.
- Let's have a trust survey!
  - Unique **Organization** field.

- Subject: C=ES, CN=Autoridad de Certificacion Firmaprofesional CIF A62634068
- Subject: C=EU, L=Madrid (see current address at www.camerfirma.com/address)/serialNumber=A82743287, O=AC Camerfirma S.A., CN=Global Chambersign Root - 2008
- Subject: C=EU, O=AC Camerfirma SA CIF A82743287, OU=http://www.chambersign.org, CN=Chambers of Commerce Root
- Subject: CN=ACCVRAIZ1, OU=PKIACCV, O=ACCV, C=ES
- Subject: C=EE, O=AS Sertifitseerimiskeskus, CN=EE Certification Centre Root CA/emailAddress=pki@sk.ee

- Subject: C=IT, L=Milan, O=Actalis S.p.A./03358520967, CN=Actalis Authentication Root CA
- Subject: C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust Public CA Root
- Subject: C=US, O=AffirmTrust, CN=AffirmTrust Premium ECC
- Subject: C=ES, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), OU=Serveis Publics de Certificacio, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Jerarquia Entitats de Certificacio Catalanes, CN=EC-ACC
- Subject: CN=Atos TrustedRoot 2011, O=Atos, C=DE

- Subject: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
- Subject: C=NO, O=Buypass AS-983163327, CN=Buypass Class 2 Root CA
- Subject: C=CN, O=CNNIC, CN=CNNIC ROOT
- Subject: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Certification Authority
- Subject: C=FR, O=Certinomis, OU=0002 433998903, CN=Certinomis - Root CA

- Subject: C=FR, O=Certplus, CN=Class 2 Primary CA
- Subject: C=CN, O=China Financial Certification Authority, CN=CFCA EV ROOT
- Subject: C=CN, O=China Internet Network Information Center, CN=China Internet Network Information Center EV Certificates Root
- Subject: C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority
- Subject: CN=ComSign CA, O=ComSign, C=IL

- Subject: C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=AAA Certificate Services
- Subject: O=Cybertrust, Inc, CN=Cybertrust Global Root
- Subject: C=DE, O=D-Trust GmbH, CN=D-TRUST Root Class 3 CA 2 2009
- Subject: C=DE, O=Deutsche Telekom AG, OU=T-TeleSec Trust Center, CN=Deutsche Telekom Root CA 2
- Subject: C=DE, O=Deutscher Sparkassen Verlag GmbH, OU=S-TRUST Certification Services, CN=S-TRUST Universal Root CA

- Subject: C=FR, O=Dhimyotis, CN=Certigna
- Subject: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Assured ID Root G3
- Subject: C=US, O=Digital Signature Trust, OU=DST ACES, CN=DST ACES CA X6
- Subject: O=Digital Signature Trust Co., CN=DST Root CA X3
- Subject: C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig Root R2

- Subject: C=TR, L=Ankara, O=E-Tu\xC4\x9Fra EBG Bili\xC5\x9Fim Teknolojileri ve Hizmetleri A.\xC5\x9E., OU=E-Tugra Sertifikasyon Merkezi, CN=E-Tugra Certification Authority
- Subject: CN=ACEDICOM Root, OU=PKI, O=EDICOM, C=ES
- Subject: C=US, O=Entrust, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2009 Entrust, Inc. - for authorized use only, CN=Entrust Root Certification Authority - G2
- Subject: O=Entrust.net, OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.), OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Certification Authority (2048)
- Subject: C=ES, O=Generalitat Valenciana, OU=PKIGVA, CN=Root CA Generalitat Valenciana

- Subject: C=US, O=GeoTrust Inc., CN=GeoTrust Primary Certification Authority
- Subject: OU=GlobalSign Root CA - R3, O=GlobalSign, CN=GlobalSign
- Subject: C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA
- Subject: C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2
- Subject: C=TW, O=Government Root Certification Authority

- Subject: C=GR, L=Athens, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions RootCA 2015
- Subject: C=HK, O=Hongkong Post, CN=Hongkong Post Root CA 1
- Subject: C=ES, O=IZENPE S.A., CN=Izenpe.com
- Subject: C=US, O=IdenTrust, CN=IdenTrust Public Sector Root CA 1
- Subject: C=US, O=Internet Security Research Group, CN=ISRG Root X1

- Subject: C=JP, O=Japan Certification Services, Inc., CN=SecureSign RootCA11
- Subject: C=JP, O=Japanese Government, OU=ApplicationCA
- Subject: C=PL, O=Krajowa Izba Rozliczeniowa S.A., CN=SZAFIR ROOT CA2
- Subject: C=HU, L=Budapest, O=Microsec Ltd., OU=e-Szigno CA, CN=Microsec e-Szigno Root CA
- Subject: C=HU, L=Budapest, O=NetLock Kft., OU=Tan\xC3\xBAs\xC3\xADtv\xC3\xA1nykiad\xC3\xB3k (Certification Services), CN=NetLock Arany (Class Gold) F\xC5\x91tan\xC3\xBAs\xC3\xADtv\xC3\xA1ny

- Subject: C=US, O=Network Solutions L.L.C., CN=Network Solutions Certificate Authority
- Subject: C=FR, O=OpenTrust, CN=OpenTrust Root CA G2
- Subject: C=BM, O=QuoVadis Limited, CN=QuoVadis Root CA 3 G3
- Subject: O=RSA Security Inc, OU=RSA Security 2048 V3
- Subject: C=JP, O=SECOM Trust Systems CO.,LTD., OU=Security Communication RootCA2

- Subject: C=JP, O=SECOM Trust.net, OU=Security Communication RootCA1
- Subject: C=US, O=SecureTrust Corporation, CN=Secure Global CA
- Subject: emailAddress=contacto@procert.net.ve, L=Chacao, ST=Miranda, OU=Proveedor de Certificados PROCERT, O=Sistema Nacional de Certificacion Electronica, C=VE, CN=PSCProcert
- Subject: C=CO, O=Sociedad Cameral de Certificaci\xC3\xB3n Digital - Certic\xC3\xA1mara S.A., CN=AC Ra\xC3\xADz Certic\xC3\xA1mara S.A.
- Subject: C=FI, O=Sonera, CN=Sonera Class2 CA

- Subject: C=NL, O=Staat der Nederlanden, CN=Staat der Nederlanden EV Root CA
- Subject: C=US, ST=Arizona, L=Scottsdale, O=Starfield Technologies, Inc., CN=Starfield Root Certificate Authority - G2
- Subject: C=CH, O=SwissSign AG, CN=SwissSign Platinum CA - G2
- Subject: C=ch, O=Swisscom, OU=Digital Certificate Services, CN=Swisscom Root CA 2
- Subject: C=DE, O=T-Systems Enterprise Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 2

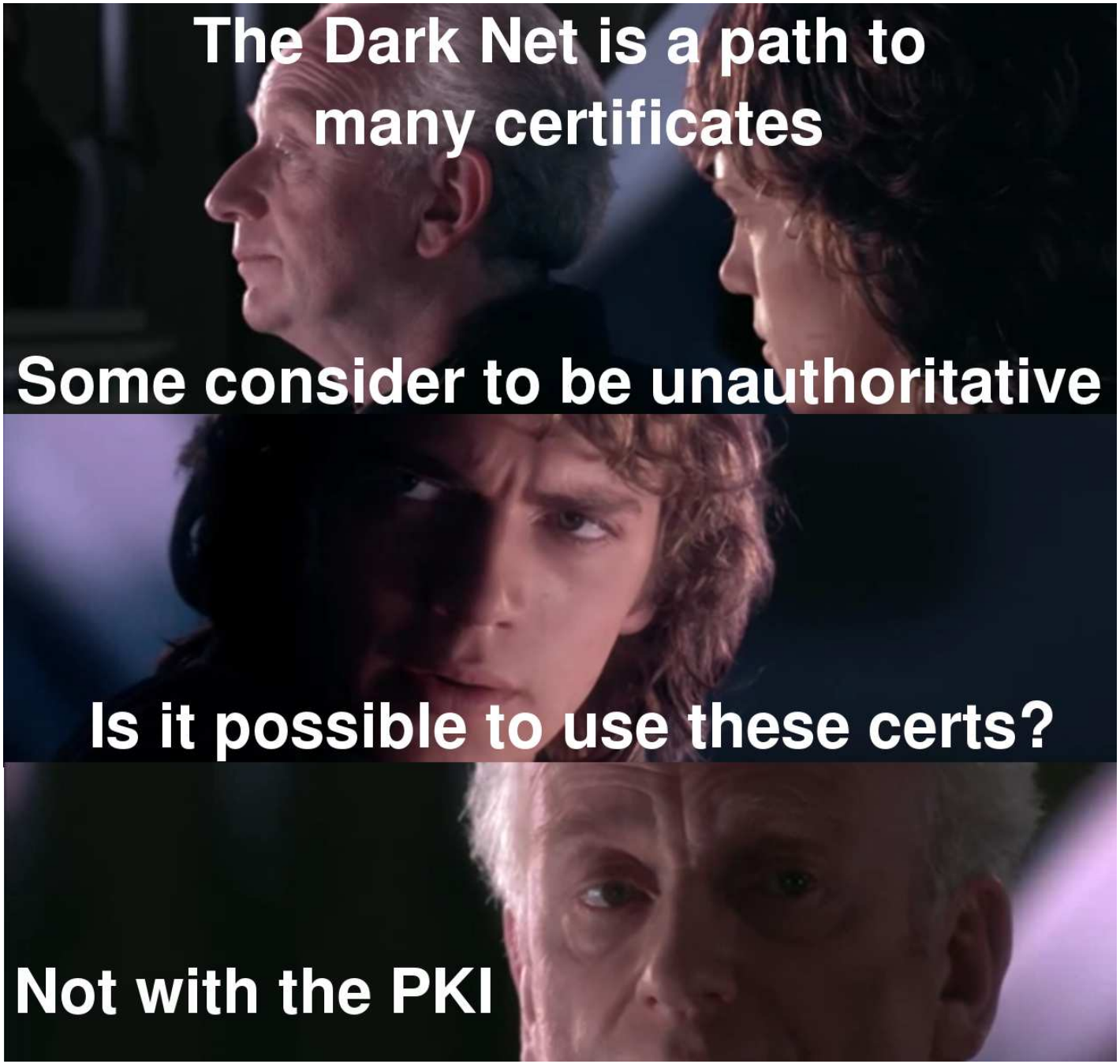
- Subject: C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Global Root CA
- Subject: C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 3 CA, CN=TC TrustCenter Class 3 CA II
- Subject: C=TR, L=Ankara, O=T\xC3\x9CRKTRUST Bilgi \xC4\xB0leti\xC5\x9Fim ve Bili\xC5\x9Fim G\xC3\xBCvenli\xC4\x9Fi Hizmetleri A.\xC5\x9E., CN=T\xC3\x9CRKTRUST Elektronik Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1 H5
- Subject: CN=T\xC3\x9CRKTRUST Elektronik Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1, C=TR, L=Ankara, O=T\xC3\x9CRKTRUST Bilgi \xC4\xB0leti\xC5\x9Fim ve Bili\xC5\x9Fim G\xC3\xBCvenli\xC4\x9Fi Hizmetleri A.\xC5\x9E. (c) Aral\xC4\xB1k 2007
- Subject: C=TR, L=Gebze - Kocaeli, O=T\xC3\xBCrkiye Bilimsel ve Teknolojik Ara\xC5\x9Ft\xC4\xB1rma Kurumu - T\xC3\x9CB\xC4\xB0TAK, OU=Ulusal Elektronik ve Kriptoloji Ara\xC5\x9Ft\xC4\xB1rma

- Subject: O=TeliaSonera, CN=TeliaSonera Root CA v1
- Subject: C=US, O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority
- Subject: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust ECC Certification Authority
- Subject: C=GB, O=Trustis Limited, OU=Trustis FPS Root CA
- Subject: C=PL, O=Unizeto Sp. z o.o., CN=Certum CA

- Subject: C=PL, O=Unizeto Technologies S.A., OU=Certum Certification Authority, CN=Certum Trusted Network CA 2
- Subject: C=US, O=VISA, OU=Visa International Service Association, CN=Visa eCommerce Root
- Subject: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G3
- Subject: C=CH, O=WISeKey, OU=OISTE Foundation Endorsed, CN=OISTE WISeKey Global Root GB CA
- Subject: C=US, O=Wells Fargo WellsSecure, OU=Wells Fargo Bank NA, CN=WellsSecure Public Root Certificate Authority

- Subject: C=CN, O=WoSign CA Limited, CN=Certification Authority of WoSign G2
- Subject: C=US, OU=www.xrampsecurity.com, O=XRamp Security Services Inc, CN=XRamp Global Certification Authority
- Subject: C=RO, O=certSIGN, OU=certSIGN ROOT CA
- Subject: C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA

- Listed root CAs, not intermediate CAs.
- "I trust browser vendors".
  - Not unreasonable.
- Might not always trust.
- Why deal with PKI ha$$le?



Outline

Subcommands

- `s_client` – Connect to SSL/TLS service.
- `x509` – Mostly reading certificates.
- `genrsa` – Generate private RSA key.
- `req` – Generate Certificate Signing Requests (CSRs).
- `ca` – Sign CSRs.
- `verify` – Test certificate authentication.

- `man` pages no `openssl` prefix (ex: `man x509`).

Get Server Cert.

- Use `s_client`.
- Example for `google.com`: '`openssl s_client -showcerts -connect google.com:443`'.
  - `-showcerts` show intermediate certs (else only "leaf" cert).
  - `-connect <address>:<port>`.
  - SIGINT to close connection (`^C`).
  - Yank cert(s) via X clipboard (or ugly `sed`).


-----BEGIN CERTIFICATE-----
MIIH4jCCBsqgAwIBAgIIRKcjuLex9iIwDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
BhMCVVMxEzARBgNVBAoTCkdvb2dsZSBJbmMxJTAjBgNVBAMTHEdvb2dsZSBJbnRl
cm5ldCBBdXRob3JpdHkgRzIwHhcNMTcwMzIyMTY1NDE5WhcNMTcwNjE0MTYxNzAw
WjBmMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwN
TW91bnRhaW4gVmlldzETMBEGA1UECgwKR29vZ2xlIEluYzEVMBMGA1UEAwwMKi5n
b29nbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAk0vBWQrk
knSwN4OiCEmOysOQiBnikCVL+3pJpl494KhAhV/wfBc79fkcMQJtMNNmeciH33i5
hjv6OmfGXV/lt32pqzHlsi41PZ+OGSeHxXXYkmth2GIzgkA1dvUKe2xpOIDEqFST
AItouAHXLYT/ixhQMLZzVqGL1hIbrvL9XDmddf7KWyuwk/eNJX1fPWIXePmgVUIr
qYhdGAp+P/QEl0BpCubGhrvdC7h7ewwh/1bJp0auVPNDS/IeN1rFMz09IvngkVK6
bMSbVNgneOXRWiZFoq6MHqw9EemE5vbG1ulHhkP/RIatu/a/bLMgPBC8npzzavr3
OJ8vgPM7Bu6V5QIDAQABo4IErzCCBKswHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsG
AQUFBwMCMIIDewYDVR0RBIIDcjCCA26CDCouZ29vZ2xlLmNvbYINKi5hbmRyb2lk
LmNvbYIWKi5hcHBlbmdpbmUuZ29vZ2xlLmNvbYISKi5jbG91ZC5nb29nbGUuY29t
gg4qLmdjcC5ndnQyLmNvbYIWKi5nb29nbGUtYW5hbHl0aWNzLmNvbYILKi5nb29n
bGUuY2GCCyouZ29vZ2xlLmNsgg4qLmdvb2dsZS5jby5pboIOKi5nb29nbGUuY28u
anCCDiouZ29vZ2xlLmNvLnVrgg8qLmdvb2dsZS5jb20uYXKCDyouZ29vZ2xlLmNv
bS5hdYIPKi5nb29nbGUuY29tLmJygg8qLmdvb2dsZS5jb20uY2+CDyouZ29vZ2xl
LmNvbS5teIIPKi5nb29nbGUuY29tLnRygg8qLmdvb2dsZS5jb20udm6CCyouZ29v
Z2xlLmRlggsqLmdvb2dsZS5lc4ILKi5nb29nbGUuZnKCCyouZ29vZ2xlLmh1ggsq
Lmdvb2dsZS5pdIILKi5nb29nbGUubmyCCyouZ29vZ2xlLnBsggsqLmdvb2dsZS5w
dIISKi5nb29nbGVhZGFwaXMuY29tgg8qLmdvb2dsZWFwaXMuY26CFCouZ29vZ2xl
Y29tbWVyY2UuY29tghEqLmdvb2dsZXZpZGVvLmNvbYIMKi5nc3RhdGljLmNugg0q
LmdzdGF0aWMuY29tggoqLmd2dDEuY29tggoqLmd2dDIuY29tghQqLm1ldHJpYy5n
c3RhdGljLmNvbYIMKi51cmNoaW4uY29tghAqLnVybC5nb29nbGUuY29tghYqLnlv
dXR1YmUtbm9jb29raWUuY29tgg0qLnlvdXR1YmUuY29tghYqLnlvdXR1YmVlZHVj
YXRpb24uY29tggsqLnl0aW1nLmNvbYIaYW5kcm9pZC5jbGllbnRzLmdvb2dsZS5j
b22CC2FuZHJvaWQuY29tghtkZXZlbG9wZXIuYW5kcm9pZC5nb29nbGUuY26CBGcu
Y2+CBmdvby5nbIIUZ29vZ2xlLWFuYWx5dGljcy5jb22CCmdvb2dsZS5jb22CEmdv
b2dsZWNvbW1lcmNlLmNvbYIKdXJjaGluLmNvbYIKd3d3Lmdvby5nbIIIeW91dHUu
YmWCC3lvdXR1YmUuY29tghR5b3VOdWJ1ZWR1Y2FOaW9uLmNvbTBoBggrBgEFBQcB
AQRcMFowKwYIKwYBBQUHMAKGH2h0dHA6Ly9wa2kuZ29vZ2xlLmNvbS9HSUFHMi5j
cnQwKwYIKwYBBQUHMAGGH2h0dHA6Ly9jbGllbnRzMS5nb29nbGUuY29tL29jc3Aw
HQYDVR0OBBYEFKu4h6ibdbH2OMiy/azE+mOLPsLMMAwGA1UdEwEB/wQCMAAwHwYD
VR0jBBgwFoAUStOGFhu89mi1dvWBtrtiGrpagS8wIQYDVR0gBBowGDAMBgorBgEE
AdZ5AgUBMAgGBmeBDAECAjAwBgNVHR8EKTAnMCWgI6Ahhh9odHRwOi8vcGtpLmdv
b2dsZS5jb20vR0lBRzIuY3JsMA0GCSqGSIb3DQEBCwUAA4IBAQBdFuOMx2S0ygRC
64gBdEh6xQZr7h42hN+UlGoDCkiQ9ygXBPfXA4nPBxpuSqoiCdUX05Cw8yP8GW2o
ZM+mbqKA9CrWlLTmnOJCO4zpzJmgncVRbXTbPL4xJl1pcIZSU5+aRG8TvWsFzg+h
EdDiRdI9wwSmaHB3eAFrBioJfKTljAkiK+zO1Lv4apM96Z19/FMAOGmUZzL6agMg
g9yki+K7lcJR7UYM7AsZOoUDAJfk1Wd3JDbzPYc+tqJCTuSrO/ohevR/9v2xlvJT
QdljfksCJvQTsIsOJBSbaE7ST6hGaMCdISXy6GlmVEdqbMGbDPSvwcaXcnW+RN4j
pIrNZkxw
-----END CERTIFICATE-----

View Cert.

- Two formats: DER and PEM.
  - DER $\approx$ GPG (binary)
  - PEM $\approx$ ASC (text)
- Use `x509`.
- Example: `openssl x509 -in cert.pem -text`
  - `-in <file>` cert. to read.
  - `-text` output cert's text.
  - Use `-inform der` if DER format.
  - Use `-noout` to not print PEM cert.

```
frostsnow@localhost ~ $ openssl x509 -in the_googles.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            44:a7:23:b8:b7:b1:f6:22
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Google Inc, CN=Google Internet Authority G2
        Validity
            Not Before: Mar 22 16:54:19 2017 GMT
            Not After : Jun 14 16:17:00 2017 GMT
        Subject: C=US, ST=California, L=Mountain View, O=Google Inc, CN=*.google.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:93:4b:c1:59:0a:e4:92:74:b0:37:8d:22:08:49:
                    b4:ca:cd:10:88:19:e2:90:25:4b:fb:7a:49:a6:5e:
                    3d:e0:a8:40:85:5f:f0:7c:17:3b:f5:f9:1c:31:02:
                    6d:30:d3:66:79:c8:87:df:78:b9:86:3b:fa:3a:67:
                    c6:5d:5f:e5:b7:7d:a9:ab:31:e5:b2:2e:35:3d:9f:
                    8e:19:27:87:c5:75:d8:92:6b:61:d8:62:33:82:40:
                    35:76:f5:0a:7b:6c:69:38:80:c4:a8:54:93:00:8b:
                    68:b8:01:d7:2d:84:ff:8b:18:50:30:b6:73:56:a1:
                    8b:d6:12:1b:ae:f2:fd:5c:39:9d:75:fe:ca:5b:2b:
                    b0:93:f7:8d:25:7d:5f:3d:62:17:78:f9:a0:55:42:
                    2b:a9:88:5d:18:0a:7e:3f:f4:04:97:40:69:0a:e6:
                    c6:86:bb:dd:0b:b8:7b:7b:0c:21:ff:56:c9:a7:46:
                    ae:54:f3:43:4b:f2:1e:37:5a:c5:33:3d:3d:22:f9:
                    e0:91:52:ba:6c:c4:9b:54:d8:27:78:e5:d1:5a:26:
                    45:a2:ae:8c:1e:ac:3d:11:e9:84:e6:f6:c6:d6:e9:
                    47:86:43:ff:44:86:ad:bb:f6:bf:6c:b3:20:3c:10:
                    bc:9e:9c:f3:6a:fa:f7:d0:9f:2f:80:f3:3b:06:ee:
                    95:e6
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                DNS:*.google.com, DNS:*.android.com, DNS:*.appengine.google.com, DNS:*.cloud.google.com, DNS:*.gcp.gvt2.com, DNS:*.google-analytics.com, DNS:*.google.ca, DNS:*.google.cl, DNS:*.google.co.in, DNS:*
.google.co.jp, DNS:*.google.co.uk, DNS:*.google.com.ar, DNS:*.google.com.au, DNS:*.google.com.br, DNS:*.google.com.co, DNS:*.google.com.mx, DNS:*.google.com.tr, DNS:*.google.com.vn, DNS:*.google.de, DNS:*.google.
es, DNS:*.google.fr, DNS:*.google.hu, DNS:*.google.it, DNS:*.google.nl, DNS:*.google.pl, DNS:*.google.pt, DNS:*.googleadapis.com, DNS:*.googleapis.cn, DNS:*.googlecommerce.com, DNS:*.googlevideo.com, DNS:*.gstati
c.cn, DNS:*.gstatic.com, DNS:*.gvt1.com, DNS:*.gvt2.com, DNS:*.metric.gstatic.com, DNS:*.urchin.com, DNS:*.url.google.com, DNS:*.youtube-nocookie.com, DNS:*.youtube.com, DNS:*.youtubeeducation.com, DNS:*.ytimg.co
m, DNS:android.clients.google.com, DNS:android.com, DNS:developer.android.google.cn, DNS:g.co, DNS:goo.gl, DNS:google-analytics.com, DNS:google.com, DNS:googlecommerce.com, DNS:urchin.com, DNS:www.goo.gl, DNS:you
tu.be, DNS:youtube.com, DNS:youtubeeducation.com
            Authority Information Access:
                CA Issuers - URI:http://pki.google.com/GIAG2.crt
                OCSP - URI:http://clients1.google.com/ocsp

            X509v3 Subject Key Identifier:
                AB:B8:87:A8:9B:75:B1:F6:D0:C8:B2:FD:AC:C4:FA:63:8B:3E:C2:CC
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Authority Key Identifier:
                keyid:4A:DD:06:16:1B:BC:F6:68:B5:76:F5:81:B6:BB:62:1A:BA:5A:81:2F

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.11129.2.5.1
                Policy: 2.23.140.1.2.2

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://pki.google.com/GIAG2.crl

    Signature Algorithm: sha256WithRSAEncryption
         5d:16:e3:8c:c7:64:b4:ca:04:42:eb:88:01:74:48:7a:c5:06:
         6b:ee:1e:36:84:df:94:94:6a:03:0a:48:90:f7:28:17:04:f7:
         d7:03:89:cf:07:1a:6e:4a:aa:22:09:d5:17:d3:90:b0:f3:23:
         [illegible]
```

```
frostsnow@localhost ~ $ openssl x509 -in the_googles.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            44:a7:23:b8:b7:b1:f6:22
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, O=Google Inc, CN=Google Internet Authority G2
        Validity
            Not Before: Mar 22 16:54:19 2017 GMT
            Not After : Jun 14 16:17:00 2017 GMT
    Subject: C=US, ST=California, L=Mountain View, O=Google Inc, CN=*.google.com
```

Self-signed cert. pt. 1

- Two steps[5]:
  - Generate key.
  - Generate self-signed cert.
- Pt. 1: use `genrsa`.
- `umask 0077; openssl genrsa -out key.pem 4096`
  - `umask 0077` – Unix DAC.
  - `-out key.pem` – Send to file `key.pem`.
  - 4096 – RSA key size.
  - Key is **unencrypted**.
  - Optional: `-aes256` to encrypt the key.

[5] May be combined into one step, but it's ugly.

```
frostsnow@localhost ~ $ umask 0077; openssl genrsa -out key.pem 4096
Generating RSA private key, 4096 bit long modulus
.........++
..............++
e is 65537 (0x10001)
```

- Pt. 2: use `req`.
- `openssl req -x509 -key key.pem -out cert.pem -days 7200 -sha512`
  - `-x509` – Self-signed cert.
  - `-key key.pem` – Input private key.
  - `-out cert.pem` – Output to `cert.pem`.
  - `-days 7200` – Expiration time (default: one month, ick!).
  - `-sha512` – Stronger signature algorithm (default: SHA-256).

```
frostsnow@localhost ~ $ openssl req -x509 -key key.pem -out cert.pem -days 7200 -sha512
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:.
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) [Internet Widgits Pty Ltd]:.
Organizational Unit Name (eg, section) []:.
Common Name (e.g. server FQDN or YOUR name) []:Dumbledrumpf
Email Address []:.
```

```
frostsnow@localhost ~ $ openssl x509 -in cert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            e0:e5:b6:31:2e:c3:8f:11
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=Dumbledrumpf
        Validity
            Not Before: Apr  7 02:04:05 2017 GMT
            Not After : Dec 23 02:04:05 2036 GMT
        Subject: CN=Dumbledrumpf
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:e3:83:fc:e5:cc:00:ba:f5:81:8e:38:3f:89:45:
                    49:39:84:87:d4:89:7d:d8:8a:0a:2c:b7:4d:7b:c0:
                    f6:5f:1d:72:02:a2:0d:fd:be:d8:71:5d:c7:48:0c:
                    ed:4c:b0:51:32:ae:78:4a:fc:44:55:65:82:aa:1d:
                    23:18:6f:6a:91:44:e0:30:a9:7a:42:e3:8d:eb:52:
                    ac:9f:ff:9a:a1:57:e6:12:80:d9:16:8a:93:2f:91:
                    8b:a3:f5:2d:0f:57:3d:50:c9:00:cd:de:a6:84:73:
                    a8:6b:61:0a:e4:93:21:44:9a:8d:b9:ea:b6:00:ef:
                    aa:81:eb:20:0a:82:7f:dc:53:d1:a3:6c:bd:41:8e:
                    d1:7b:63:6f:21:1f:78:6c:ae:37:ad:3c:15:21:04:
                    c6:d3:4b:23:c4:08:52:bb:cc:41:40:4e:2b:07:40:
                    78:1f:c1:19:31:42:36:93:e4:ec:85:ff:f4:98:d0:
                    55:57:17:ad:2b:77:59:3d:88:8f:89:7a:54:58:03:
                    bc:fe:4c:ce:3d:b6:91:20:bb:94:59:f4:9b:39:7a:
                    47:bc:7b:dd:2d:31:d8:35:a6:d3:6c:22:6d:43:0b:
                    38:8a:0e:ee:93:16:93:d3:ca:d3:51:bf:16:83:2e:
                    72:95:65:d8:e9:b1:fe:0f:8e:0c:2e:5b:cb:e6:d5:
                    b8:bc:34:5f:51:5a:6d:38:4a:60:6c:dd:ca:ee:3a:
                    4f:8f:df:08:b5:5d:1d:be:f5:b0:86:b8:28:9f:51:
                    e2:47:40:24:fe:91:ef:c4:d2:2a:6b:70:0b:48:f1:
                    ef:9d:24:4b:75:29:03:04:30:45:18:7b:ba:69:ce:
                    be:40:cd:59:48:f2:4f:f0:00:29:96:4a:2b:11:c0:
                    10:a3:b6:5c:de:3a:d3:7a:8b:53:db:48:d0:ee:ba:
                    0c:ed:07:c6:29:f8:dc:69:0c:e8:14:1f:bd:85:c7:
                    07:4a:39:73:f9:c4:70:f0:ec:7a:d4:36:d9:40:11:
                    dc:2a:ca:2d:94:fe:d2:2b:85:0e:65:2f:e6:17:91:
                    a9:65:c1:e0:32:59:49:5d:5d:a3:60:82:69:d0:17:
                    2d:3f:9a:57:4d:44:a8:74:2f:f5:59:7d:a3:97:cb:
                    59:f3:a1:c5:5f:b8:b2:8b:65:df:b3:fb:9c:83:8b:
                    49:49:71:e7:97:7a:f3:8a:f1:c0:f1:12:be:3f:7f:
                    3c:7c:67:d5:6d:f4:e0:8e:42:b7:9d:c4:5e:48:2c:
                    fd:88:6d:04:df:2f:03:8a:17:8d:a9:c0:f1:5e:05:
                    95:80:81:18:a5:70:18:39:a2:a1:1f:4d:08:96:37:
                    34:dd:66:0b:b3:2d:12:04:52:c8:df:26:8c:43:ee:
                    03:83:65
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                8C:F8:0F:98:7A:88:53:88:47:FC:CB:33:CD:3F:B4:79:52:AD:CD:75
            X509v3 Authority Key Identifier:
                keyid:8C:F8:0F:98:7A:88:53:88:47:FC:CB:33:CD:3F:B4:79:52:AD:CD:75

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha512WithRSAEncryption
         87:6b:0e:27:c8:80:65:d2:27:34:c8:e6:6c:ff:12:72:3f:c3:
         11:9a:d7:7a:f6:15:d5:b9:3d:a1:43:4e:46:91:29:a5:67:96:
         be:e6:91:18:68:15:4e:ae:a7:15:ea:59:ee:8f:aa:2a:e8:7c:
         34:3b:ca:7a:58:1a:22:bb:fb:e0:01:b5:db:ca:fa:f5:f1:1a:
```

Server Certificate

- Use **your own** "PKI".
- WARNING: This example sucks.
- `openssl s_client -showcerts -connect chat.freenode.net:6697`
- Place certs **and** Root CA (from `/usr/share/ca-certificates`) in `freenode.pem`.
- `/connect -ssl_cafile freenode.pem -ssl_verify chat.freenode.net 6697`

- . . . and nothing of real value was gained :(.

Client Certificate

- Using your self-signed cert.
- `umask 0077; openssl genrsa -out key.pem 4096`
- `openssl req -x509 -key key.pem -out cert.pem -days 7200 -sha512`
- `/connect -ssl_cert cert.pem -ssl_pkey key.pem chat.freenode.net 6697`
- Client cert **not** validated.
- Uses fingerprint (hash) instead.
- Other networks vary.

- Both: `/connect -ssl_cafile freenode.pem -ssl_verify -ssl_cert cert.pem -ssl_pkey key.pem chat.freenode.net 6697`
- Verifies both client **and** server.

- Questions?