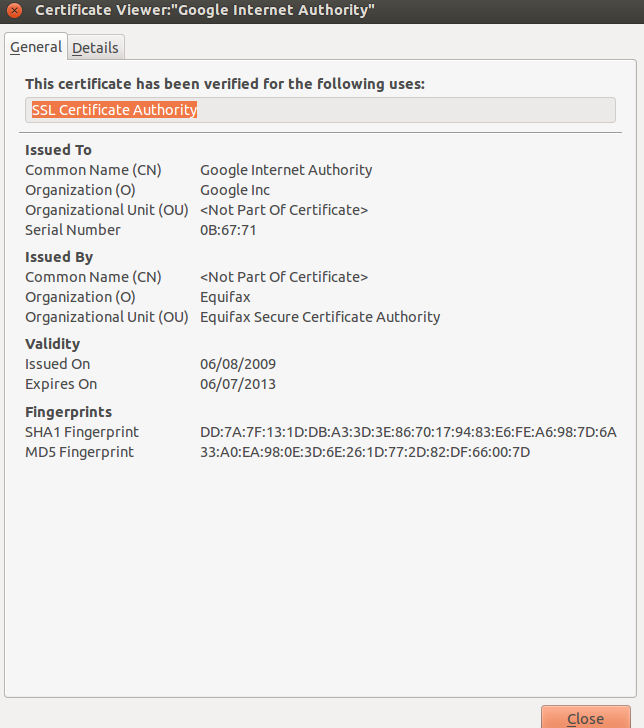
What is a SSL/TLS Certificate ?

Contents



OpenSSL to generate Certificates

#-----------------------------------Create PKI Root Certificate----------------

# Root generates key pair

openssl genrsa -out NCSU\_key\_pair.pem 1024

# Create a PKI x509 certificate

openssl req -new -x509 -keyout NCSU\_key\_pair.pem \

-out NCSU\_root\_cert.pem

# Export PKI certificate into DER format

# (DER format can be loaded into browser)

openssl x509 -in cacert.pem -outform DER -out cacert.der

#-------------------------------------Create Sub-Authority Certificate-------

#Alice generates key pair

openssl genrsa -out Alice\_key\_pair.pem 1024

# Alice creates "User Certificate Request"

openssl req -new -keyout Alice\_key\_pair.pem \

-out Alice\_usercert-req.pem

# Root CA configures CA parameters

gedit /usr/lib/ssl/openssl.cnf

# Root CA generats Alice’s Certificate

openssl ca -in Alice\_usercert-req.pem -out Alice\_usercert.pem

# To import signed certificate into browser

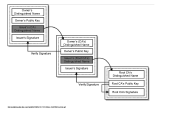
#convert to PKCS12 format

openssl pkcs12 -export -in Alice\_usercert.pem \

-inkey userkey.pem > usercert.p12

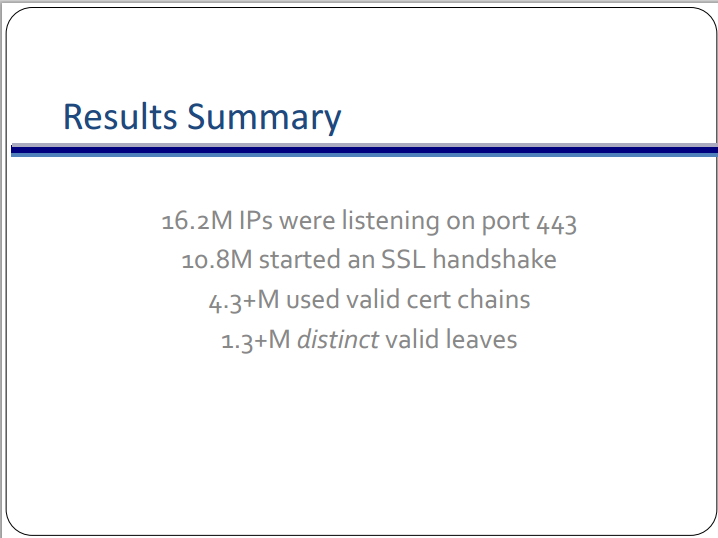
**Public Key Infrastructure**

Certificate Authority Chain of Trust



* Certificate generated by Root Authority for secondary CA
* Certificate generated by secondary CA for tertiary CA
* And so the chain grows…

2010 SSL Observatory Project



* Poster Background illustrates around 650 organizations that function as Certificate Authorities trusted(direct and indirect) by Mozilla and Microsoft

<https://www.eff.org/files/DefconSSLiverse.pdf>

Note to Yuri: You can grab the pdf slide from the site for the resolution needed.

**Security**

PKI Trust models

* Monopolistic
* Oligarchic 🡪 Currently in use
* Anarchic
* Constrain CAs to subsets

Threats to PKI

* CA chain length unrestrained
* Bugs in OpenSSL or other Certificate generating software
* Current Usage according to 2010 SSL Observatory Project
  + Changes must be widely accepted
  + Many years until certificate expiration
  + Many keys are shared