Introduction to Cryptography HW6

0616015 劉姿利

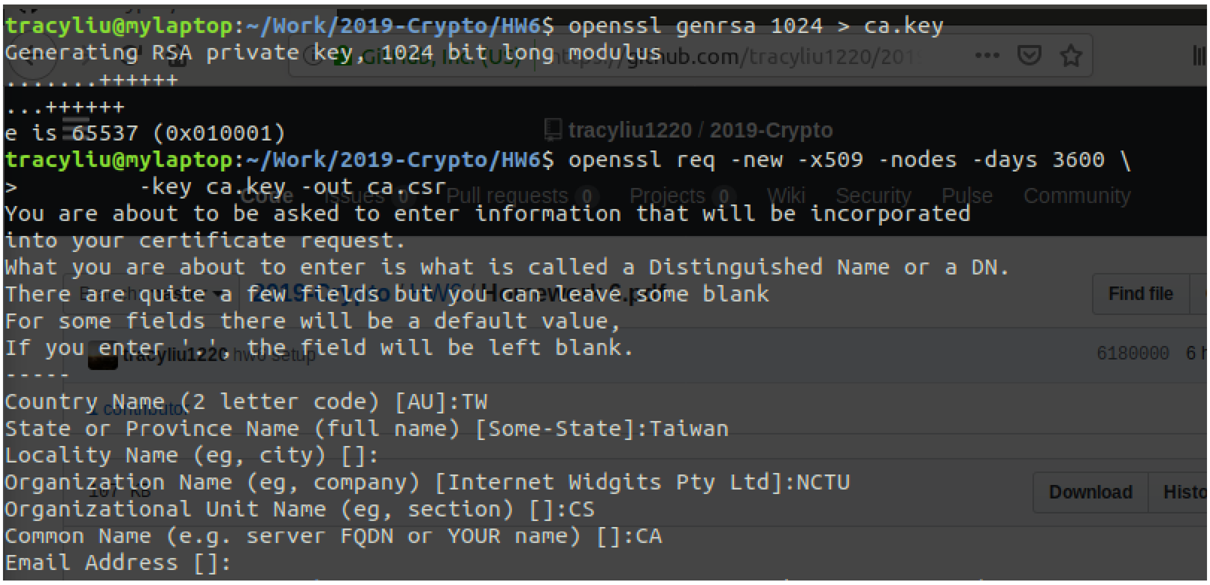
Overview

Certificate是用來證明public key擁有者的檔案，裡變包含了public key資訊、owner身份還有Certificate authority(CA)對這個檔案的digital signature。其中CA作為驗證public key以及頒發certificate的受信任的第三方。

電腦或系統可以將信任的CA資訊加到信任列表中，可以連帶信任此CA發行的digital signature，將憑證上的public key視為合法。

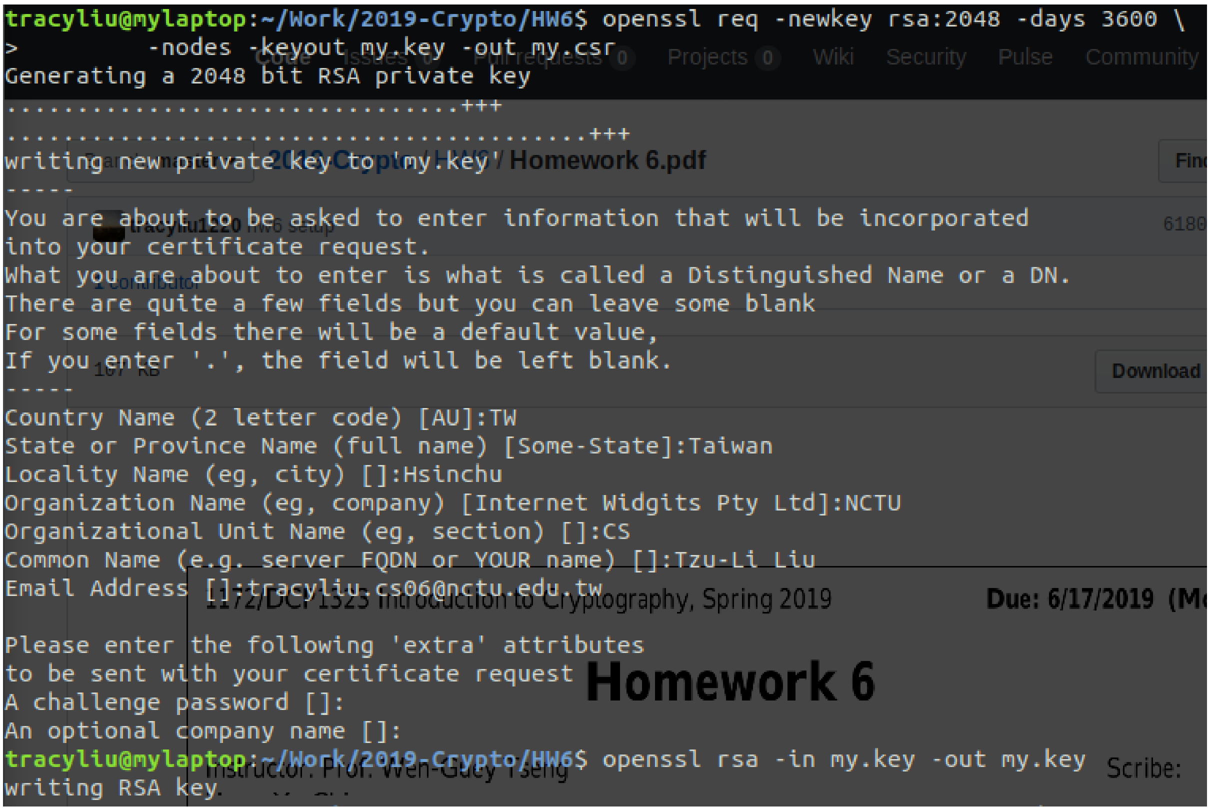
Certificates

產生ca的key和csr



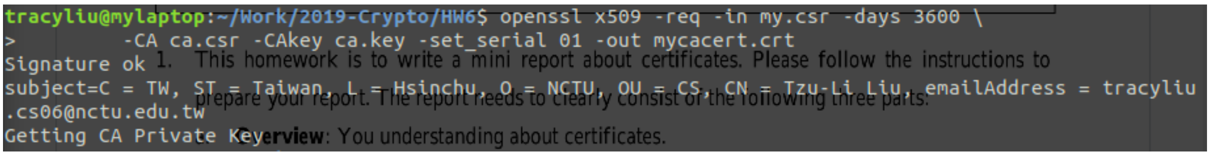
```
tracyliu@mylaptop:~/Work/2019-Crypto/HW6$ openssl genrsa 1024 > ca.key
Generating RSA private key, 1024 bit long modulus
.......++++++
...++++++
e is 65537 (0x010001)
tracyliu@mylaptop:~/Work/2019-Crypto/HW6$ openssl req -new -x509 -nodes -days 3600 \
>         -key ca.key -out ca.csr
You are about 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]:TW
State or Province Name (full name) [Some-State]:Taiwan
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NCTU
Organizational Unit Name (eg, section) []:CS
Common Name (e.g. server FQDN or YOUR name) []:CA
Email Address []:
```

產生要被簽署的key與csr



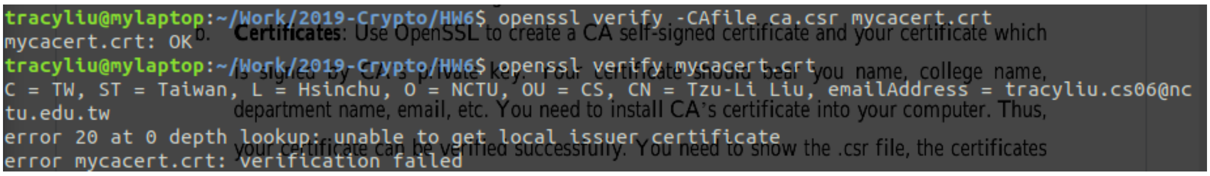
```
tracyliu@mylaptop:~/Work/2019-Crypto/HW6$ openssl req -newkey rsa:2048 -days 3600 \
>         -nodes -keyout my.key -out my.csr
Generating a 2048 bit RSA private key
.................................+++
..........................................+++
writing new private key to 'my.key'
-----
You are 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]:TW
State or Province Name (full name) [Some-State]:Taiwan
Locality Name (eg, city) []:Hsinchu
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NCTU
Organizational Unit Name (eg, section) []:CS
Common Name (e.g. server FQDN or YOUR name) []:Tzu-Li Liu
Email Address []:tracyliu.cs06@nctu.edu.tw

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
tracyliu@mylaptop:~/Work/2019-Crypto/HW6$ openssl rsa -in my.key -out my.key
writing RSA key
```

用ca的key與csr來簽屬my.csr



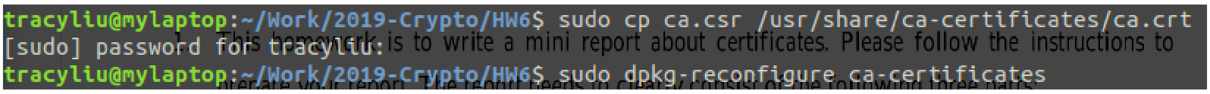
```
tracyliu@mylaptop:~/Work/2019-Crypto/HW6$ openssl x509 -req -in my.csr -days 3600 \
>         -CA ca.csr -CAkey ca.key -set_serial 01 -out mycacert.crt
Signature ok
subject=C = TW, ST = Taiwan, L = Hsinchu, O = NCTU, OU = CS, CN = Tzu-Li Liu, emailAddress = tracyliu
.cs06@nctu.edu.tw
Getting CA Private Key
```

verify，但是因為還沒將ca.csr裝到系統中所以不指定CAfile直接verify會失敗



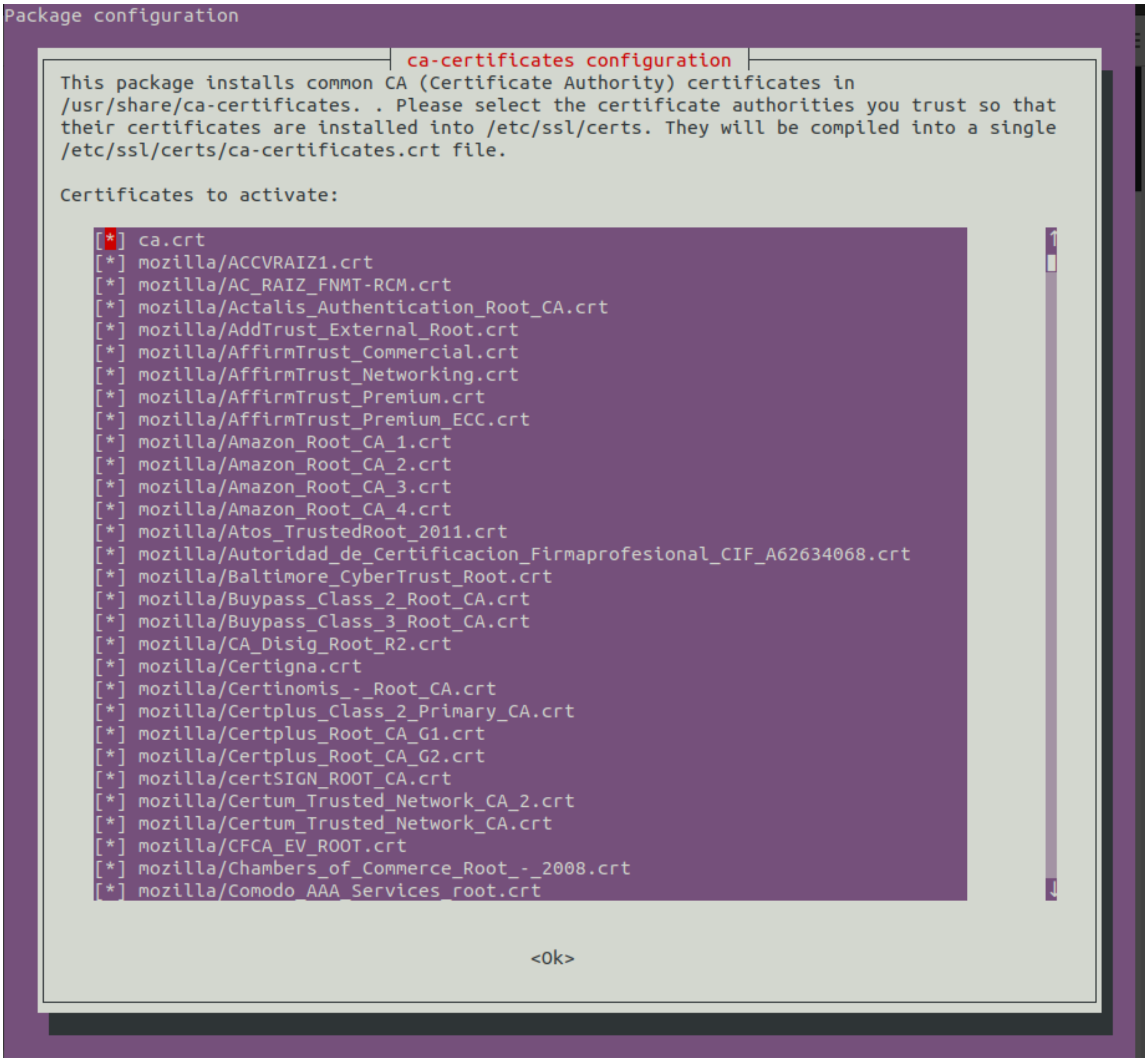
```
tracyliu@mylaptop:~/Work/2019-Crypto/HW6$ openssl verify -CAfile ca.csr mycacert.crt
mycacert.crt: OK
tracyliu@mylaptop:~/Work/2019-Crypto/HW6$ openssl verify mycacert.crt
C = TW, ST = Taiwan, L = Hsinchu, O = NCTU, OU = CS, CN = Tzu-Li Liu, emailAddress = tracyliu.cs06@nc
tu.edu.tw
error 20 at 0 depth lookup: unable to get local issuer certificate
error mycacert.crt: verification failed
```

進行安裝（ubuntu 18.04），首先要先將ca.csr移到/usr/share/ca-certificates的資料夾下，將副檔名改成.crt，然後reconfigure ca-certificates



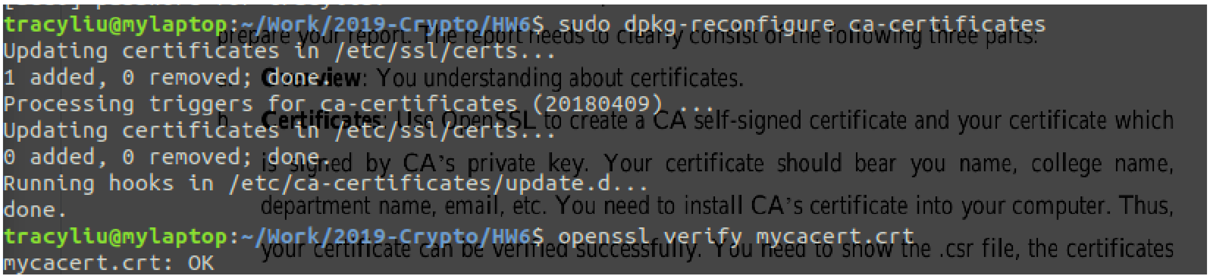
```
tracyliu@mylaptop:~/Work/2019-Crypto/HW6$ sudo cp ca.csr /usr/share/ca-certificates/ca.crt
[sudo] password for tracyliu:
tracyliu@mylaptop:~/Work/2019-Crypto/HW6$ sudo dpkg-reconfigure ca-certificates
```

reconfigure的視窗，要把ca.crt選起來



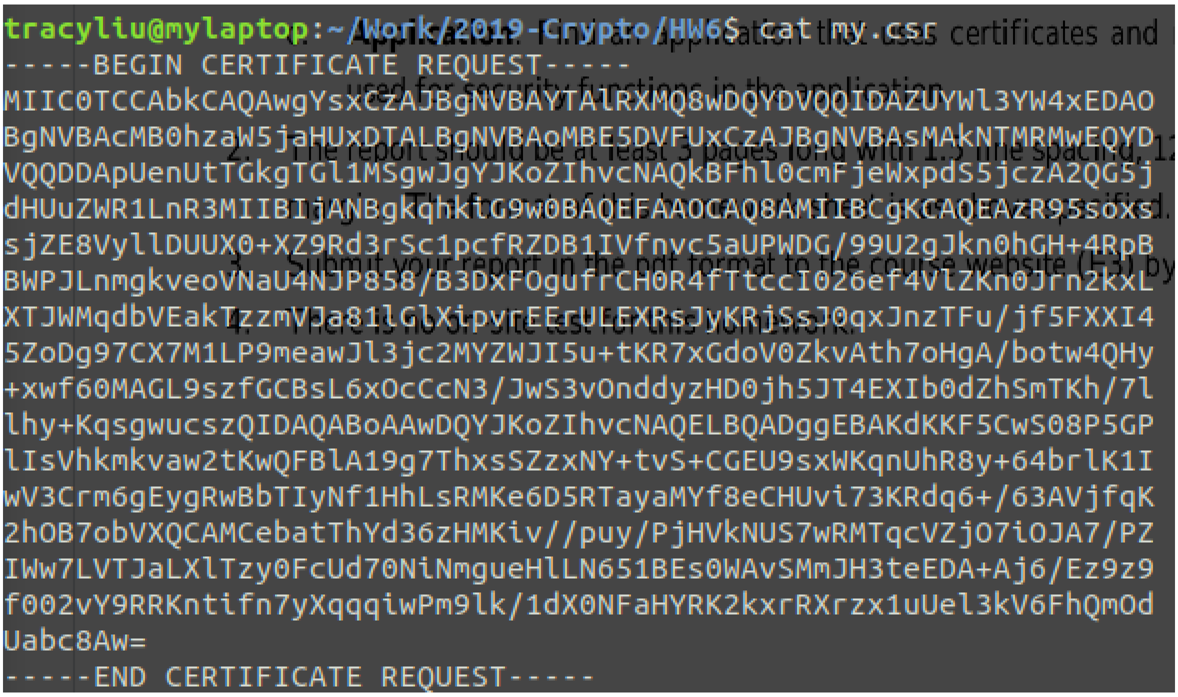
```
Package configuration

                    ca-certificates configuration

 This package installs common CA (Certificate Authority) certificates in
 /usr/share/ca-certificates. . Please select the certificate authorities you trust so that
 their certificates are installed into /etc/ssl/certs. They will be compiled into a single
 /etc/ssl/certs/ca-certificates.crt file.

 Certificates to activate:

    [*] ca.crt
    [*] mozilla/ACCVRAIZ1.crt
    [*] mozilla/AC_RAIZ_FNMT-RCM.crt
    [*] mozilla/Actalis_Authentication_Root_CA.crt
    [*] mozilla/AddTrust_External_Root.crt
    [*] mozilla/AffirmTrust_Commercial.crt
    [*] mozilla/AffirmTrust_Networking.crt
    [*] mozilla/AffirmTrust_Premium.crt
    [*] mozilla/AffirmTrust_Premium_ECC.crt
    [*] mozilla/Amazon_Root_CA_1.crt
    [*] mozilla/Amazon_Root_CA_2.crt
    [*] mozilla/Amazon_Root_CA_3.crt
    [*] mozilla/Amazon_Root_CA_4.crt
    [*] mozilla/Atos_TrustedRoot_2011.crt
    [*] mozilla/Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt
    [*] mozilla/Baltimore_CyberTrust_Root.crt
    [*] mozilla/Buypass_Class_2_Root_CA.crt
    [*] mozilla/Buypass_Class_3_Root_CA.crt
    [*] mozilla/CA_Disig_Root_R2.crt
    [*] mozilla/Certigna.crt
    [*] mozilla/Certinomis_-_Root_CA.crt
    [*] mozilla/Certplus_Class_2_Primary_CA.crt
    [*] mozilla/Certplus_Root_CA_G1.crt
    [*] mozilla/Certplus_Root_CA_G2.crt
    [*] mozilla/certSIGN_ROOT_CA.crt
    [*] mozilla/Certum_Trusted_Network_CA_2.crt
    [*] mozilla/Certum_Trusted_Network_CA.crt
    [*] mozilla/CFCA_EV_ROOT.crt
    [*] mozilla/Chambers_of_Commerce_Root_-_2008.crt
    [*] mozilla/Comodo_AAA_Services_root.crt

                                 <Ok>
```

完成reconfigure之後它會update，之後直接下verify就能成功了



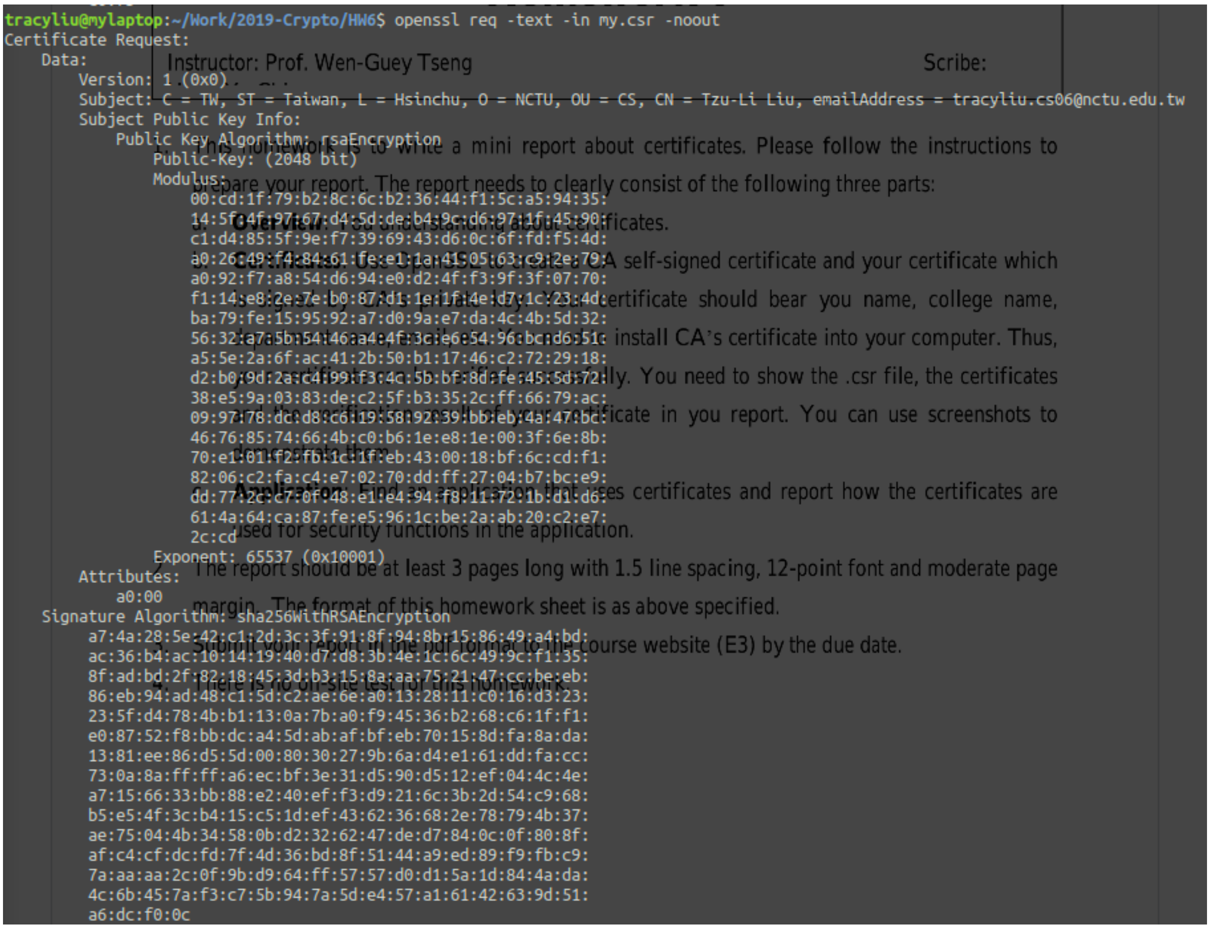
```
tracyliu@mylaptop:~/Work/2019-Crypto/HW6$ sudo dpkg-reconfigure ca-certificates
Updating certificates in /etc/ssl/certs...
1 added, 0 removed; done.
Processing triggers for ca-certificates (20180409) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
tracyliu@mylaptop:~/Work/2019-Crypto/HW6$ openssl verify mycacert.crt
mycacert.crt: OK
```

my.csr



```
tracyliu@mylaptop:~/Work/2019-Crypto/HW6$ cat my.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCAbkCAQAwgYsxCzAJBgNVBAYTAlRXMQ8wDQYDVQQIDAZUYWl3YW4xEDAO
BgNVBAcMB0hzaW5jaHUxDTALBgNVBAoMBE5DVFUxCzAJBgNVBAsMAkNTMRMwEQYD
VQQDDApUenUtTGkgTGl1MSgwJgYJKoZIhvcNAQkBFhl0cmFjeWxpdS5jczA2QG5j
dHUuZWR1LnR3MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzR95soXs
sjZE8VyllDUUX0+XZ9Rd3rSc1pcfRZDB1IVfnvc5aUPWDG/99U2gJkn0hGH+4RpB
BWPJLnmgkveoVNaU4NJP858/B3DxFOgufrCH0R4fTtccI026ef4VlZKn0Jrn2kxL
XTJWMqdbVEakTzzmVJa81lGlXipyrEErULEXRsJyKRjSsJ0qxJnzTFu/jf5FXXI4
5ZoDg97CX7M1LP9meawJl3jc2MYZWJI5u+tKR7xGdoV0ZkvAth7oHgA/botw4QHy
+xwf60MAGL9szfGCBsL6xOcCcN3/JwS3vOnddyzHD0jh5JT4EXIb0dZhSmTKh/7l
lhy+KqsgwucszQIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAKdKKF5CwS08P5GP
lIsVhkmkvaw2tKwQFBlA19g7ThxsSZzxNY+tvS+CGEU9sxWKqnUhR8y+64brlK1I
wV3Crm6gEygRwBbTIyNf1HhLsRMKe6D5RTayaMYf8eCHUvi73KRdq6+/63AVjfqK
2hOB7obVXQCAMCebatThYd36zHMKiv//puy/PjHVkNUS7wRMTqcVZjO7iOJA7/PZ
IWw7LVTJaLXlTzy0FcUd70NiNmgueHlLN651BEs0WAvSMmJH3teEDA+Aj6/Ez9z9
f002vY9RRKntifn7yXqqqiwPm9lk/1dX0NFaHYRK2kxrRXrzx1uUel3kV6FhQmOd
Uabc8Aw=
-----END CERTIFICATE REQUEST-----
```

my.csr中的內容



```
tracyliu@mylaptop:~/Work/2019-Crypto/HW6$ openssl req -text -in my.csr -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = TW, ST = Taiwan, L = Hsinchu, O = NCTU, OU = CS, CN = Tzu-Li Liu, emailAddress = tracyliu.cs06@nctu.edu.tw
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:cd:1f:79:b2:8c:6c:b2:36:44:f1:5c:a5:94:35:
                    14:5f:4f:97:67:d4:5d:de:b4:9c:d6:97:1f:45:90:
                    c1:d4:85:5f:9e:f7:39:69:43:d6:0c:6f:fd:f5:4d:
                    a0:26:49:f4:84:61:fe:e1:1a:41:05:63:c9:2e:79:
                    a0:92:f7:a8:54:d6:94:e0:d2:4f:f3:9f:3f:07:70:
                    f1:14:e8:2e:7e:b0:87:d1:1e:1f:4e:d7:1c:23:4d:
                    ba:79:fe:15:95:92:a7:d0:9a:e7:da:4c:4b:5d:32:
                    56:32:a7:5b:54:46:a4:4f:3c:e6:54:96:bc:d6:51:
                    a5:5e:2a:6f:ac:41:2b:50:b1:17:46:c2:72:29:18:
                    d2:b0:9d:2a:c4:99:f3:4c:5b:bf:8d:fe:45:5d:72:
                    38:e5:9a:03:83:de:c2:5f:b3:35:2c:ff:66:79:ac:
                    09:97:78:dc:d8:c6:19:58:92:39:bb:eb:4a:47:bc:
                    46:76:85:74:66:4b:c0:b6:1e:e8:1e:00:3f:6e:8b:
                    70:e1:01:f2:fb:1c:1f:eb:43:00:18:bf:6c:cd:f1:
                    82:06:c2:fa:c4:e7:02:70:dd:ff:27:04:b7:bc:e9:
                    dd:77:2c:c7:0f:48:e1:e4:94:f8:11:72:1b:d1:d6:
                    61:4a:64:ca:87:fe:e5:96:1c:be:2a:ab:20:c2:e7:
                    2c:cd
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         a7:4a:28:5e:42:c1:2d:3c:3f:91:8f:94:8b:15:86:49:a4:bd:
         ac:36:b4:ac:10:14:19:40:d7:d8:3b:4e:1c:6c:49:9c:f1:35:
         8f:ad:bd:2f:82:18:45:3d:b3:15:8a:aa:75:21:47:cc:be:eb:
         86:eb:94:ad:48:c1:5d:c2:ae:6e:a0:13:28:11:c0:16:d3:23:
         23:5f:d4:78:4b:b1:13:0a:7b:a0:f9:45:36:b2:68:c6:1f:f1:
         e0:87:52:f8:bb:dc:a4:5d:ab:af:bf:eb:70:15:8d:fa:8a:da:
         13:81:ee:86:d5:5d:00:80:30:27:9b:6a:d4:e1:61:dd:fa:cc:
         73:0a:8a:ff:ff:a6:ec:bf:3e:31:d5:90:d5:12:ef:04:4c:4e:
         a7:15:66:33:bb:88:e2:40:ef:f3:d9:21:6c:3b:2d:54:c9:68:
         b5:e5:4f:3c:b4:15:c5:1d:ef:43:62:36:68:2e:78:79:4b:37:
         ae:75:04:4b:34:58:0b:d2:32:62:47:de:d7:84:0c:0f:80:8f:
         af:c4:cf:dc:fd:7f:4d:36:bd:8f:51:44:a9:ed:89:f9:fb:c9:
         7a:aa:aa:2c:0f:9b:d9:64:ff:57:57:d0:d1:5a:1d:84:4a:da:
         4c:6b:45:7a:f3:c7:5b:94:7a:5d:e4:57:a1:61:42:63:9d:51:
         a6:dc:f0:0c
```

Application - DNSSEC

DNS上的信任機制是使用DNSSEC來實作certificate的

首先要先generate出KSK跟ZSK兩個keys

接著用KSK和ZSK對zonefile簽署（下圖的例子為對sec.0616015.nasa簽署）

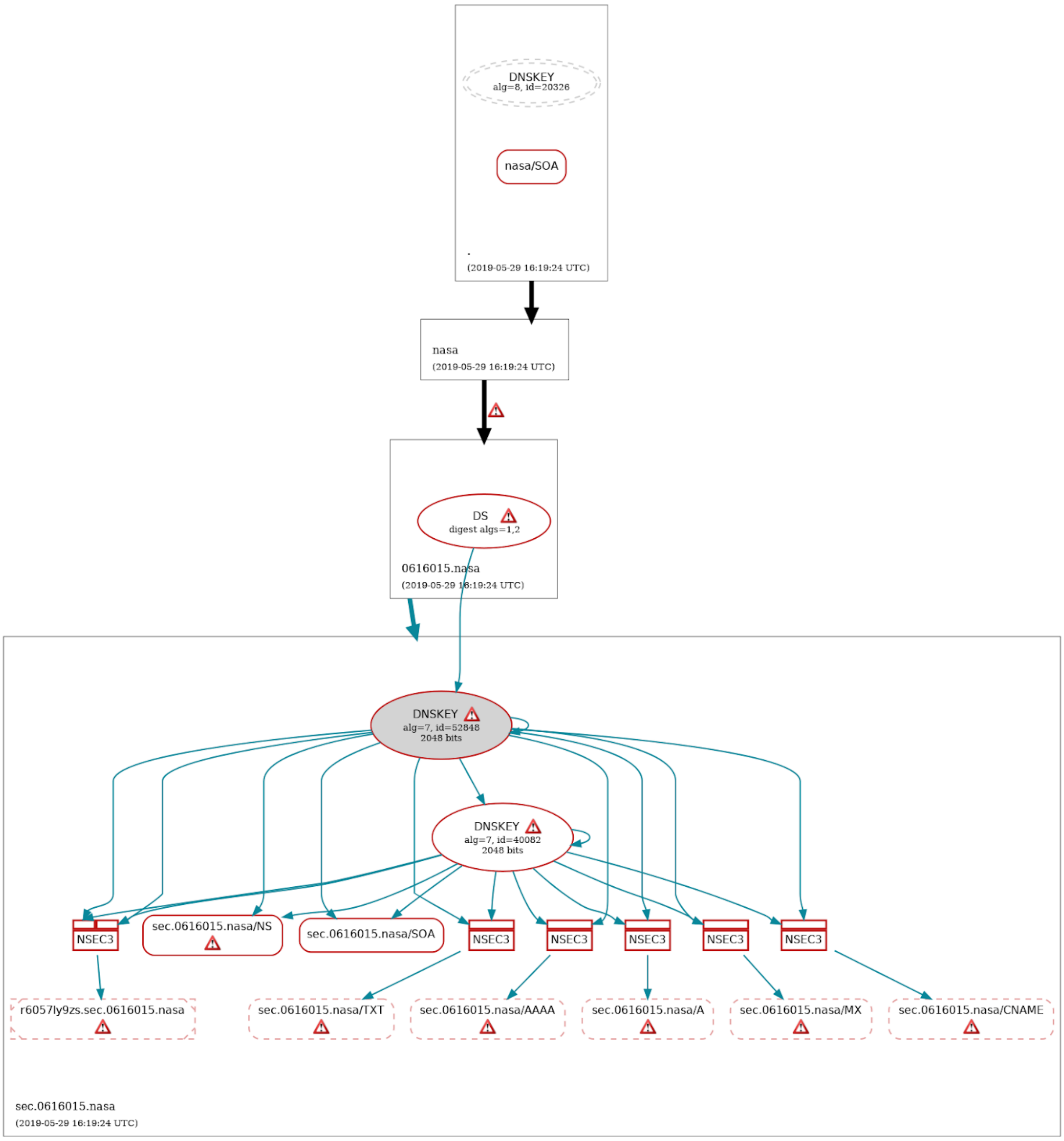
並產生出DS record

然後將DS record新增到上層domain的zonefile中

（下圖的例子上層domain的zonefile為0616015.nasa）

並再對上層的domain產生keys並簽署

代表上層能驗證public keys



圖中由0616015.nasa指向sec.0616015.nasa的綠色箭頭即為上層domain對下層domain的信任鏈