Certificate Chain

臺灣大學計資中心

網路組

游子興

Certificate Authority & Certificate

Certificate Authority(CA)
憑證簽證機關

- Root CA: Issue Certificate to CA
- Intermediate CA: Issue Certificate to Non-CA
- 重要欄位
  - Subject
    - commonName(CN)
    - organizationName(O)
    - countryName(C)
  - Public Key
  - Certificates: 憑證 → 代表 CA 有效日期
  - Issued Certificates:已簽發之憑證
  - Trust: Support OS/Browser
  - Parent CAs：based on Certificates
  - Child CAs: based on Issued Certificates

Certificate : CA 簽發之憑證

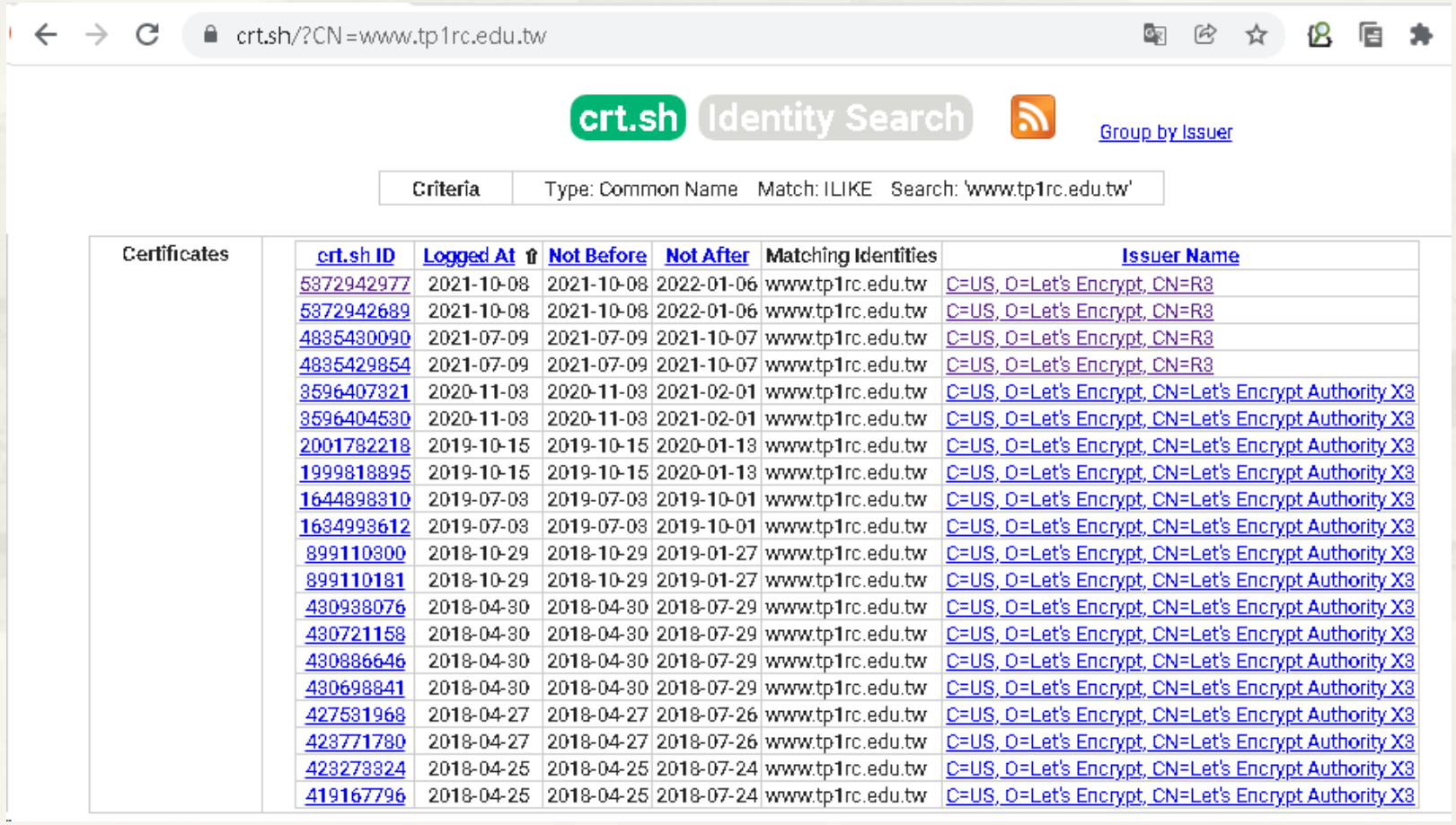
- Root Certificate
  - Self-signed (有效期: 20 ~25年)
- Intermediate Certificate
  - Signed by Root CA (有效期:5年) 可能在 Root Level
- Leaf Certificate
  - Signed by Intermediate CA (有效期: 1年)
- ※ Cross-signed: For Root/Intermediate Certificate: Signed by 同 Level CA
- 重要欄位
  - Issuer: 簽發者
    - commonName(CN)
    - organizationName(O)
    - countryName(C)
  - Validity: 有效日期
    - Not Before
    - Not After
  - Subject:主體/發給誰/Owner
    - commonName(CN)
    - organizationName(O)
    - countryName(C)

Certificate Search Engine https://crt.sh

- 記錄分兩種
  - CA or Certificate
- Domain Name,
  - https://crt.sh/?CN=www.tp1rc.edu.tw
  - https://crt.sh/?CN=*.ntu.edu.tw
- 任意關鍵字
  - Organization Name
    - National Taiwan University
  - Serial Number
    - 03:34:d3:01:86:14:a3:22:e0:a4:bb:61:a4:ab:dc:c3:bc:a3
  - Certificate Fingerprint
    - 8a7e113f8d31828dea37a650986724a9308fdd6a

Server Certificate History

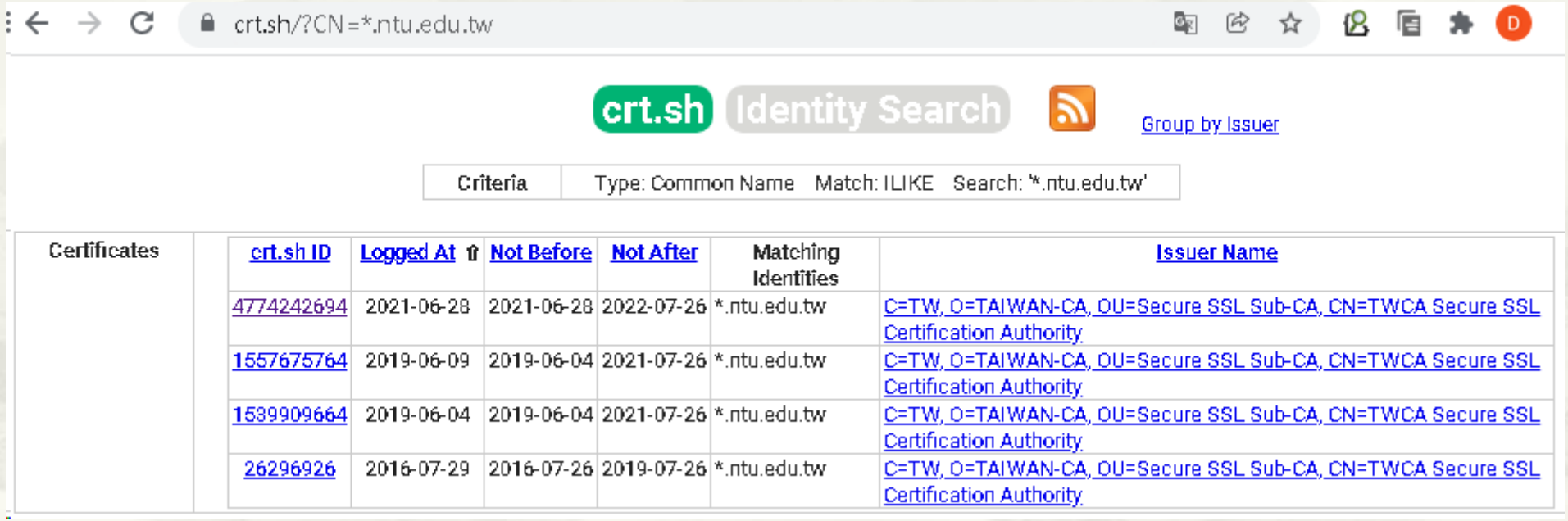
* https://crt.sh/?CN=www.tp1rc.edu.tw



crt.sh ID	Logged At ⇑	Not Before	Not After	Matching Identities	Issuer Name
5372942977	2021-10-08	2021-10-08	2022-01-06	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=R3
5372942689	2021-10-08	2021-10-08	2022-01-06	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=R3
4835430090	2021-07-09	2021-07-09	2021-10-07	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=R3
4835429854	2021-07-09	2021-07-09	2021-10-07	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=R3
3596407321	2020-11-03	2020-11-03	2021-02-01	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3596404530	2020-11-03	2020-11-03	2021-02-01	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2001782218	2019-10-15	2019-10-15	2020-01-13	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1999818895	2019-10-15	2019-10-15	2020-01-13	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1644898310	2019-07-03	2019-07-03	2019-10-01	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1634993612	2019-07-03	2019-07-03	2019-10-01	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
899110300	2018-10-29	2018-10-29	2019-01-27	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
899110181	2018-10-29	2018-10-29	2019-01-27	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
430938076	2018-04-30	2018-04-30	2018-07-29	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
430721158	2018-04-30	2018-04-30	2018-07-29	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
430886646	2018-04-30	2018-04-30	2018-07-29	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
430698841	2018-04-30	2018-04-30	2018-07-29	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
427531968	2018-04-27	2018-04-27	2018-07-26	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
423771780	2018-04-27	2018-04-27	2018-07-26	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
423273324	2018-04-25	2018-04-25	2018-07-24	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
419167796	2018-04-25	2018-04-25	2018-07-24	www.tp1rc.edu.tw	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Server Certificate History

* https://crt.sh/?CN=*.ntu.edu.tw



Root Certificate

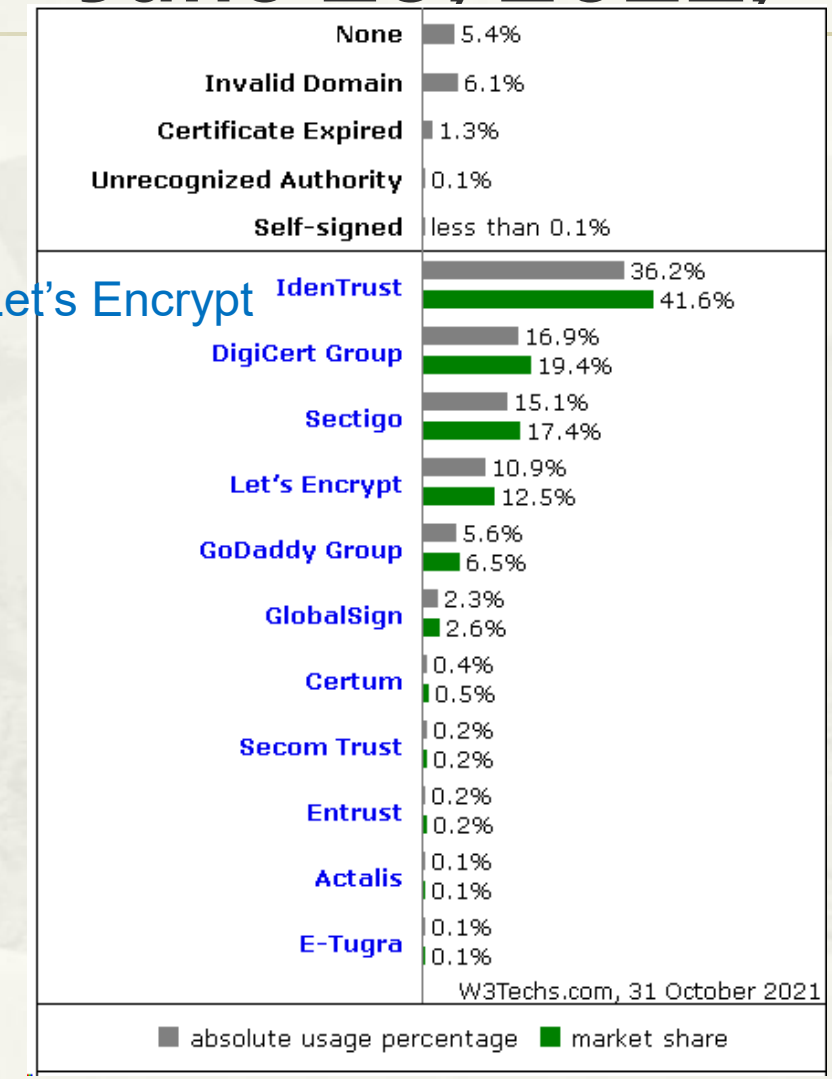
Root CA

- Server Certificate 的源頭都是由「受信任的根憑證頒發機構(trusted certificate authority)」又稱Root CA所簽發。而Root CA自身的憑證就叫作「根憑證」(root certificate).
- 根憑證沒有更上層的機構簽發，所以是自己簽發自己的憑證，屬於自簽憑證 (Self-signed).
- Root CA之所以可信任是因為其必須滿足各大作業系統(Microsoft, Apple)、瀏覽器(Chrome, Mozilla)廠商制定的 root ca program（根憑證計畫），只有滿足計畫的CA憑證才會列入廠商的 root store。
- 作業系統或瀏覽器出廠時會預載根憑證及隨付的公開金鑰(public key)。存放根憑證的地方稱為 root store/trust store.

How to Become a Trusted Certificate Authority (Public CA)

- You Must Meet Many Criteria From Different Operating Systems & Browsers
  - Microsoft Root Certificate Program
  - Apple Root Certificate Program
  - Chromium Project Root Certificate Program
  - Mozilla's CA and Root Store Programs
- You Must Invest Immense Resources (Time, Money & People)
- Your Public Root CA Requires Significant Distribution Efforts
  - it's a major process to get all the browsers, operating systems and applications to trust your certificates
- Ref. https://www.thesslstore.com/blog/how-to-become-a-certificate-authority/

Public CAs Market Share June 29, 2021.



Let's Encrypt

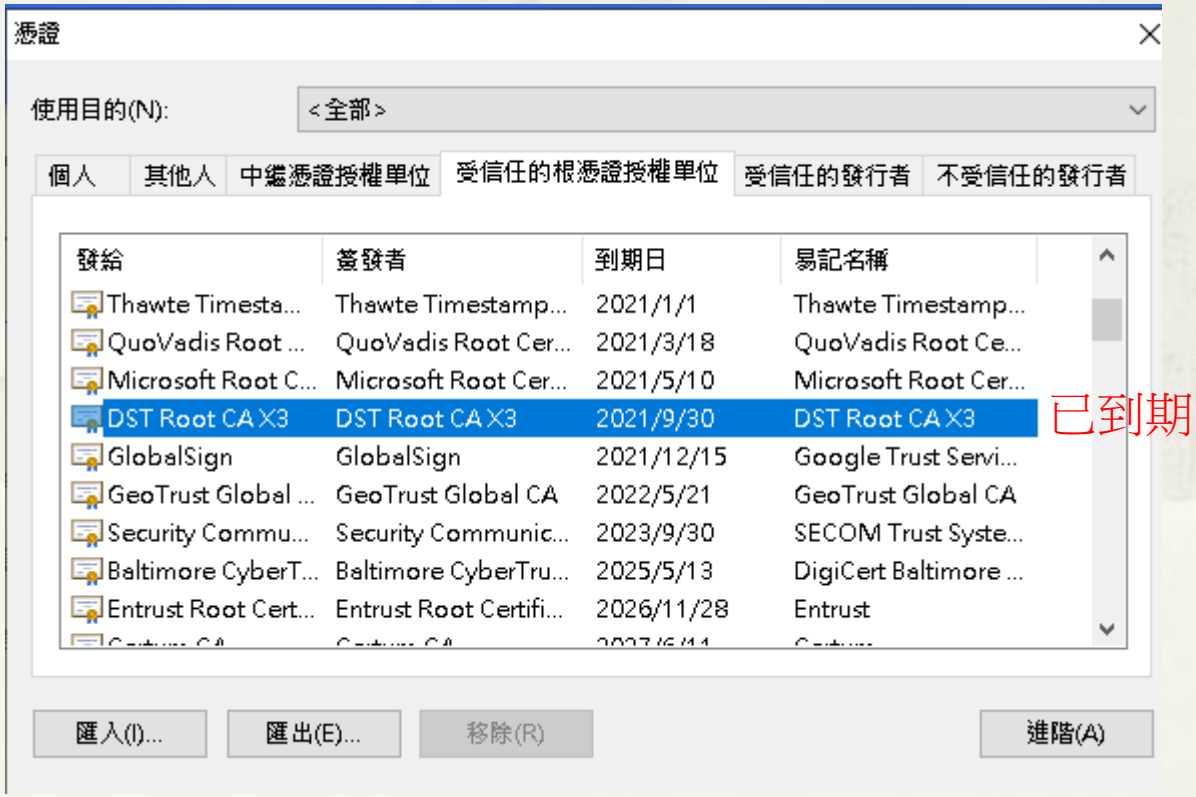
https://w3techs.com/technologies/overview/ssl_certificate

Root Store for Browsers

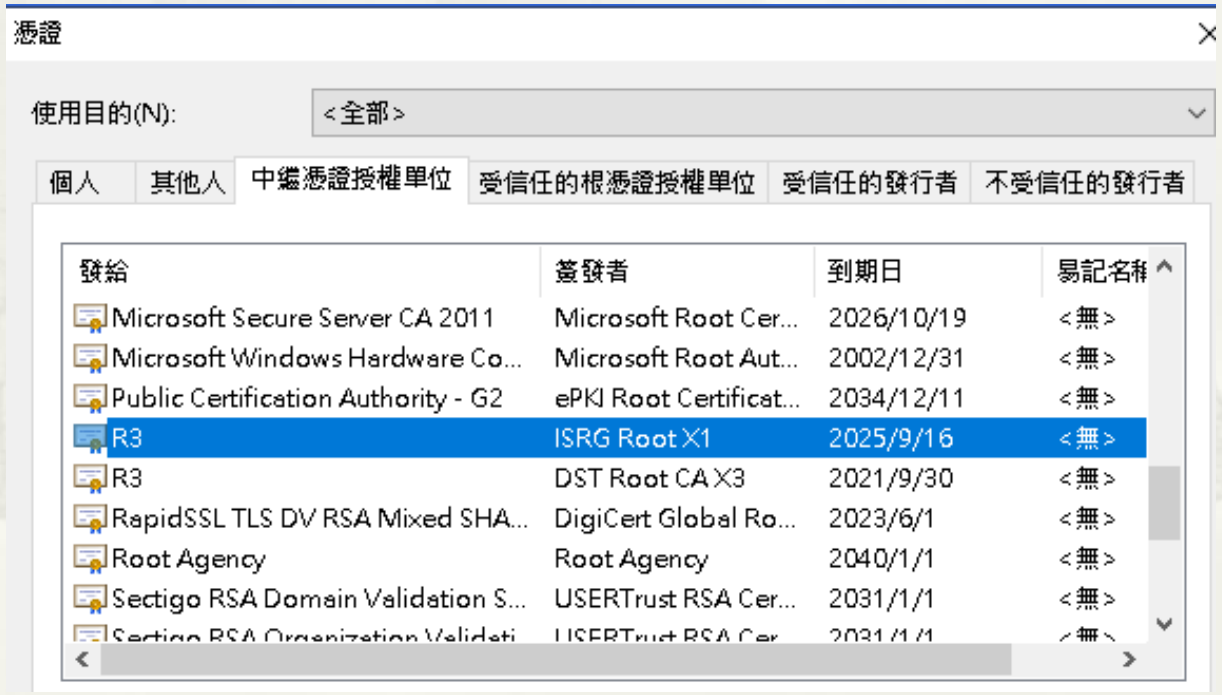
* Browsers (Chrome, Safari, Edge, Opera) generally trust the same root certificates as the operating system they are running on.
* Firefox is the exception: it has its own root store.
* Soon, new versions of Chrome will also have their own root store.
  * https://www.chromium.org/Home/chromium-security/root-ca-policy

Root Store for Chrome

* chrome://settings/security > 管理憑證

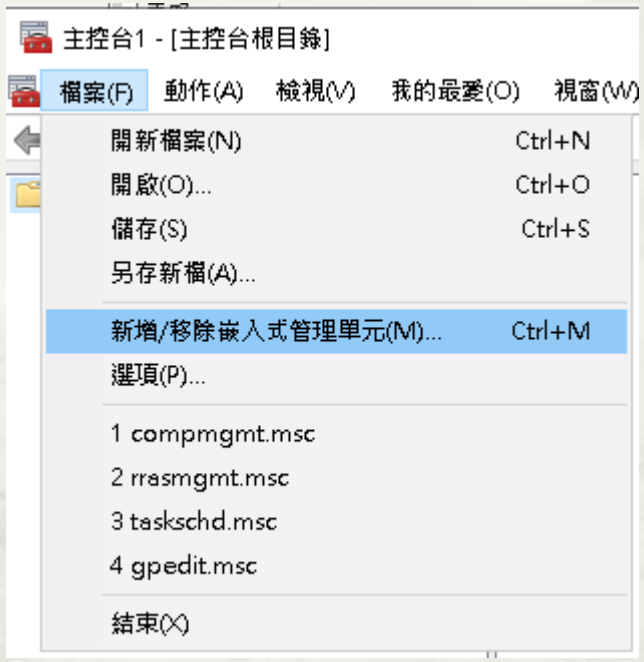


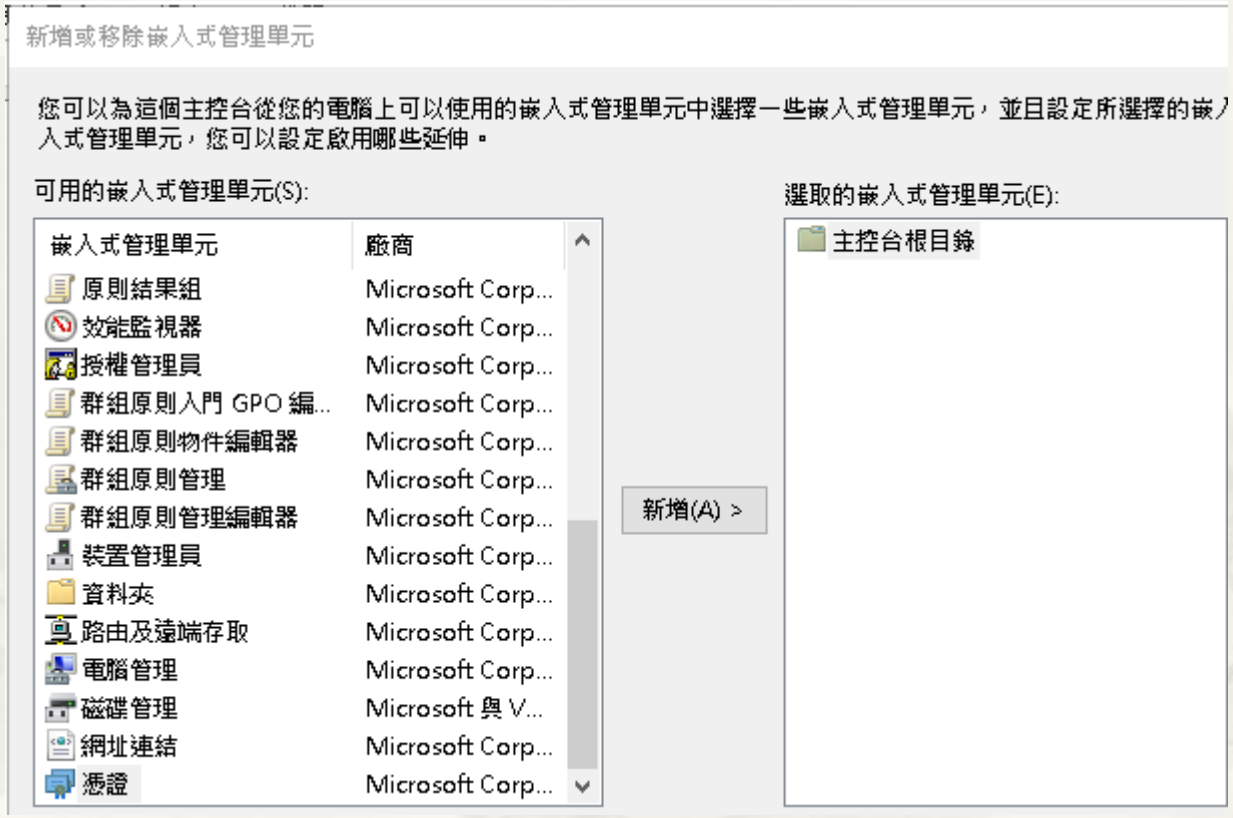
已到期



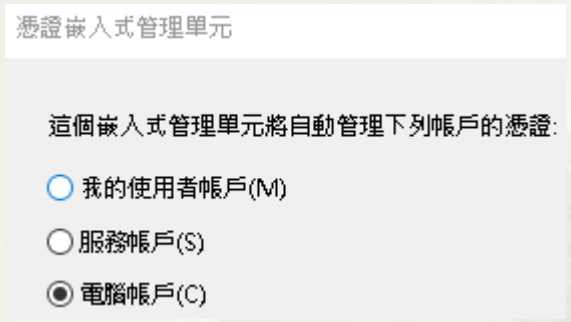
Root Store for Windows10

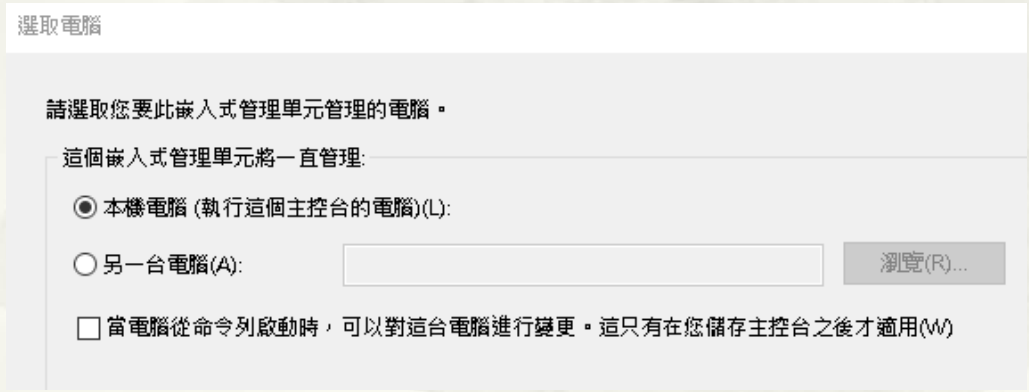
* 開始 -> 執行: mmc

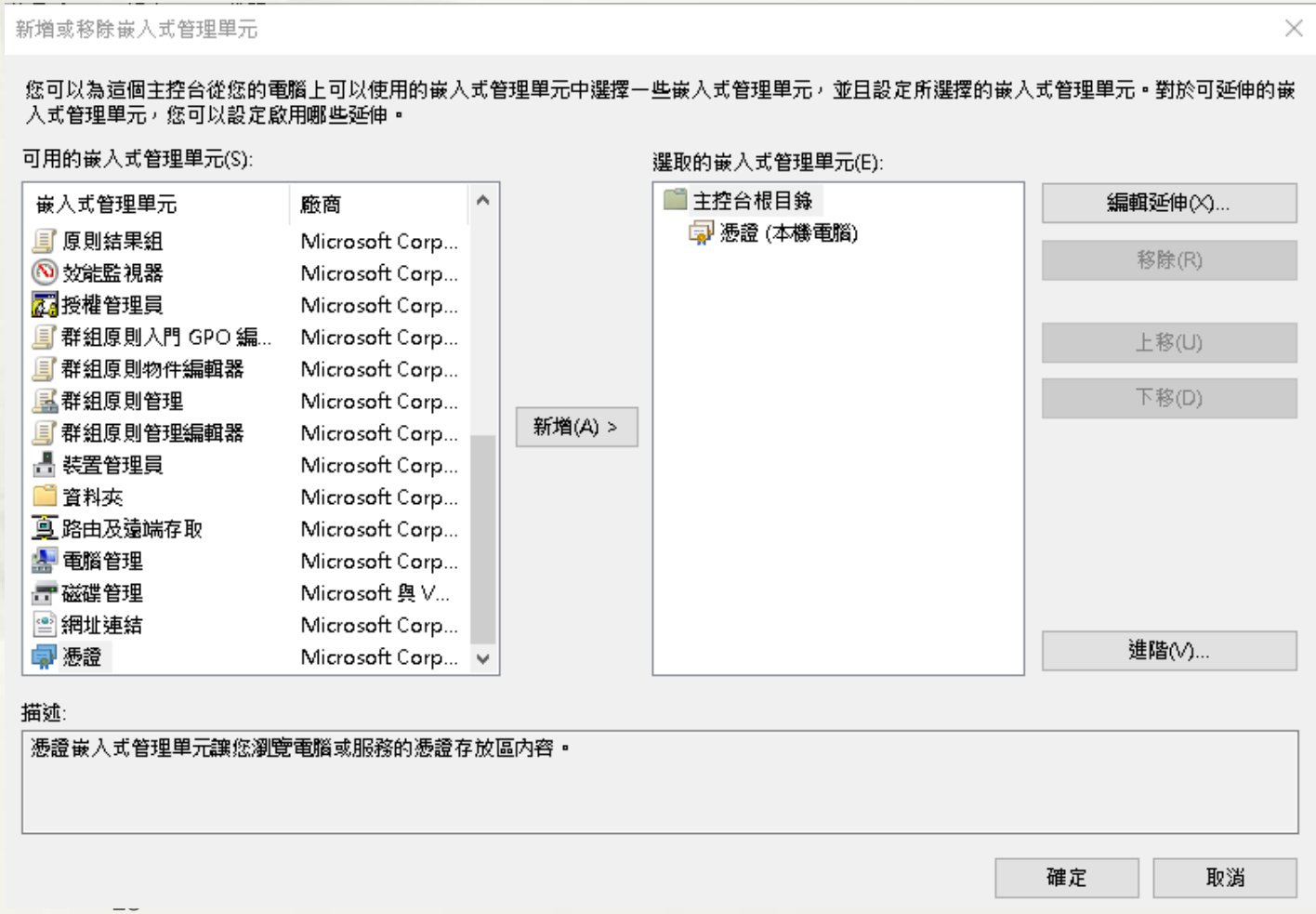




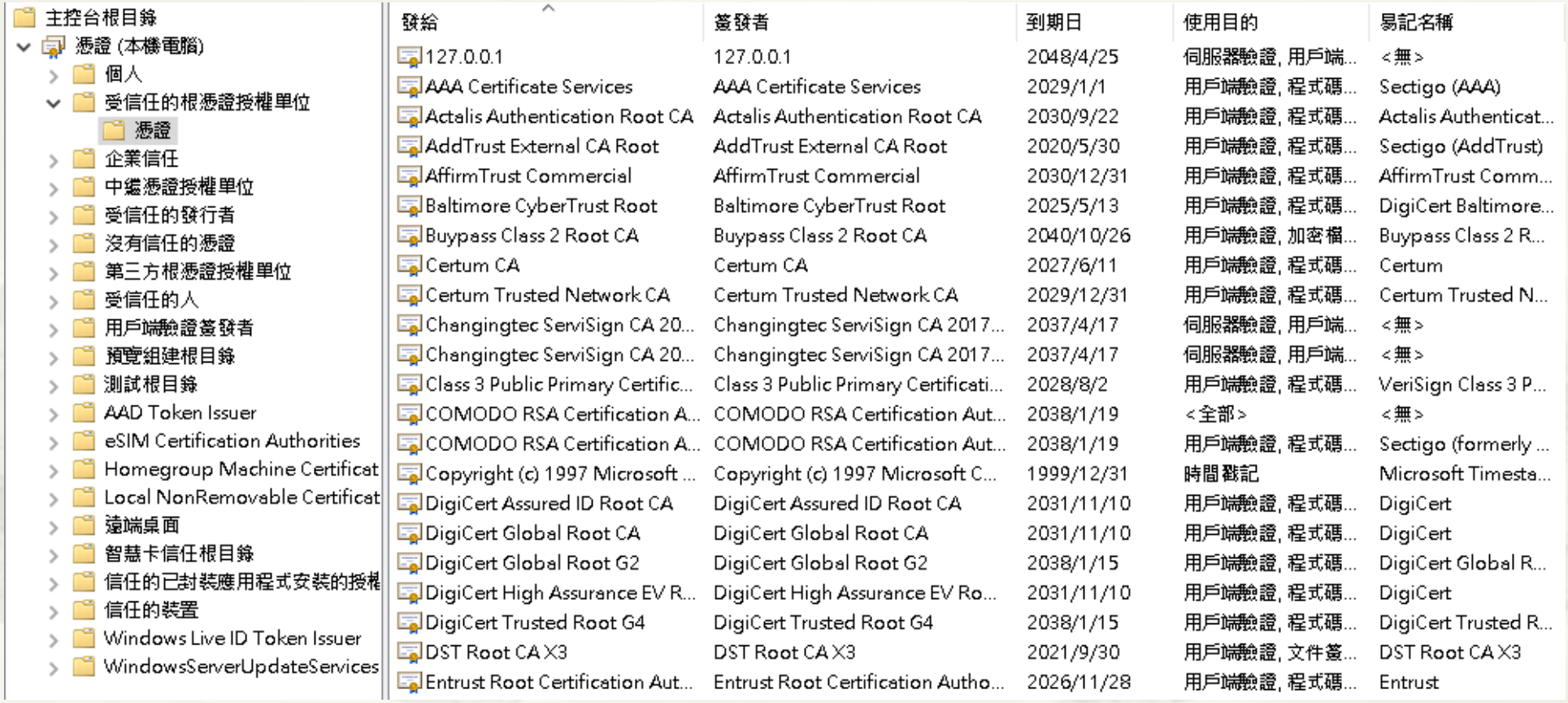
Root Store for Windows10







Root Store for Windows10



Root Store for curl

* curl -v https://www.ntu.edu.tw
* Windows

```
D:\curl-7.79.1-win64-mingw\bin>curl -v https://www.ntu.edu.tw
*   Trying 140.112.8.116:443...
* Connected to www.ntu.edu.tw (140.112.8.116) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
*  CAfile: D:\curl-7.79.1-win64-mingw\bin\curl-ca-bundle.crt
* TLSv1.0 (OUT), TLS header, Certificate Status (22):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS header, Certificate Status (22):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS header, Certificate Status (22):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS header, Finished (20):
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS header, Finished (20):
* TLSv1.2 (IN), TLS header, Certificate Status (22):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-GCM-SHA384
```

* Ubuntu20.04

```
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: /etc/ssl/certs
} [5 bytes data]
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
} [512 bytes data]
  0     0    0     0    0     0      0      0 --:--:-- --:--:-
{ [102 bytes data]
* TLSv1.2 (IN), TLS handshake, Certificate (11):
{ [6004 bytes data]
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
{ [333 bytes data]
* TLSv1.2 (IN), TLS handshake, Server finished (14):
{ [4 bytes data]
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
} [70 bytes data]
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
} [1 bytes data]
* TLSv1.2 (OUT), TLS handshake, Finished (20):
} [16 bytes data]
* TLSv1.2 (IN), TLS handshake, Finished (20):
{ [16 bytes data]
* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-GCM-SHA384
```

Root Store for Ubuntu

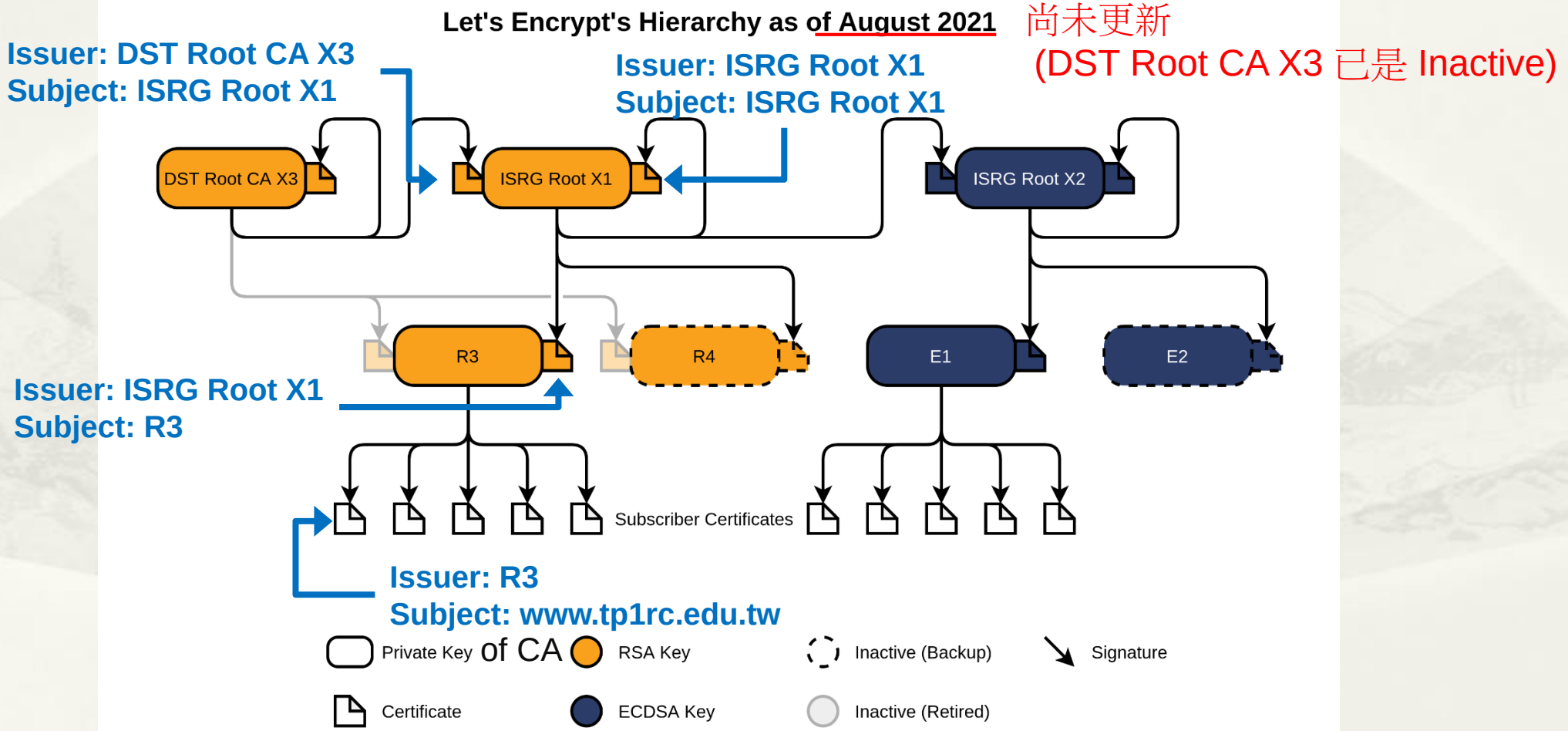
- /etc/ssl/certs/ca-certificates.crt
- apt install p11-kit
- trust list
  - pkcs11:id=%D2%87%B4%E3%DF%37%27%93%55%F6%56%EA%81%E5%36%CC%8C%1E%3F%BD;type=cert
    - type: certificate
    - label: ACCVRAIZ1
    - trust: anchor
    - category: authority
  - pkcs11:id=%F7%7D%C5%FD%C4%E8%9A%1B%77%64%A7%F5%1D%A0%CC%BF%87%60%9A%6D;type=cert
    - type: certificate
    - label: AC RAIZ FNMT-RCM
    - trust: anchor
    - category: authority
  - pkcs11:id=%52%D8%88%3A%C8%9F%78%66%ED%89%F3%7B%38%70%94%C9%02%02%36%D0;type=cert
    - type: certificate
    - label: Actalis Authentication Root CA
    - trust: anchor
    - category: authority

Certificate Chain

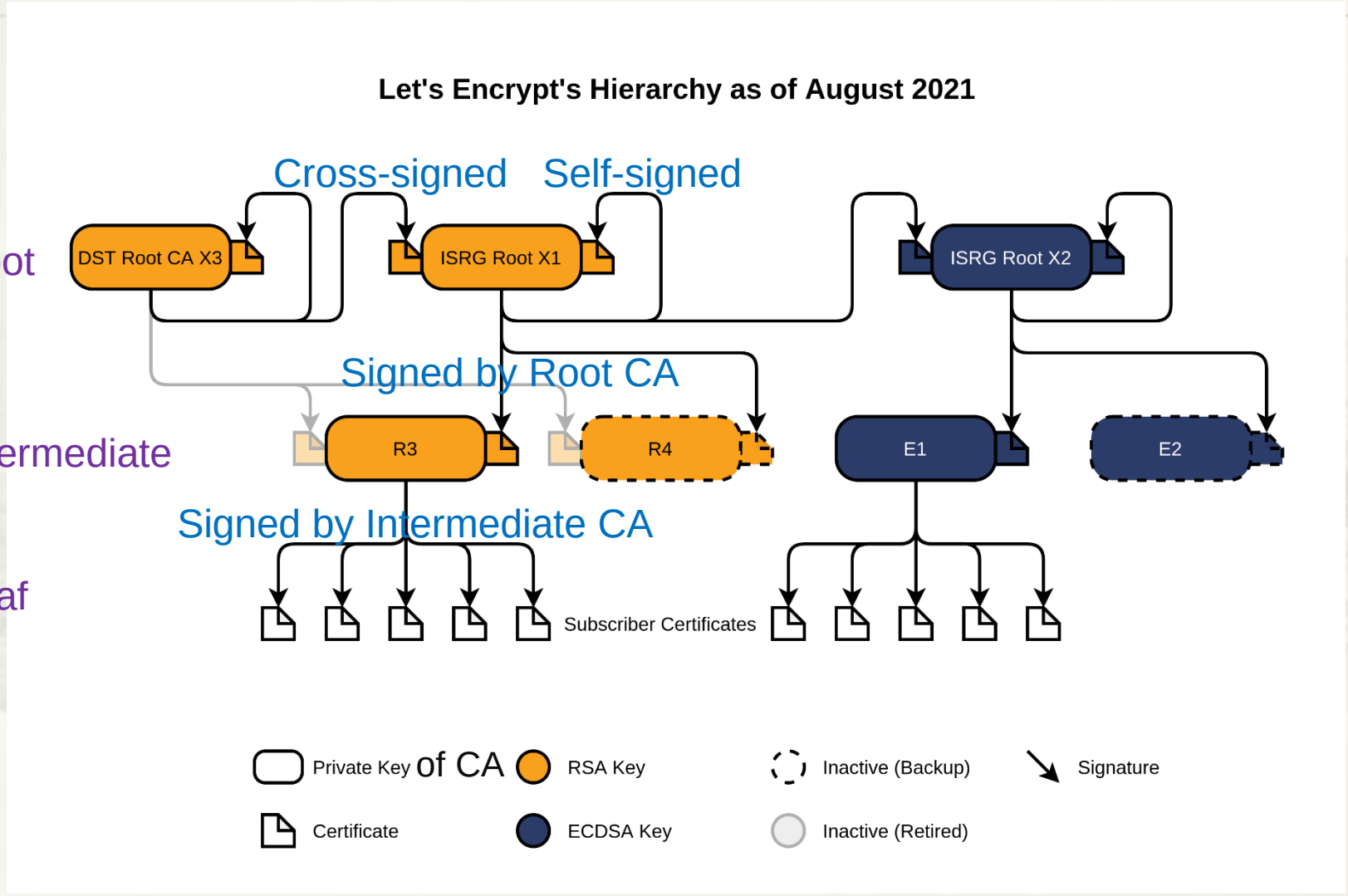
Certificate Chain
www.ntu.edu.tw

Let's Encrypt Chain of Trust

https://letsencrypt.org/certificates/



Let's Encrypt Chain of Trust



Leaf Certificate (Server Certificate) CN=www.tp1rc.edu.tw

* https://crt.sh/?id=5372942977

Server Certificate Download (PEM format)

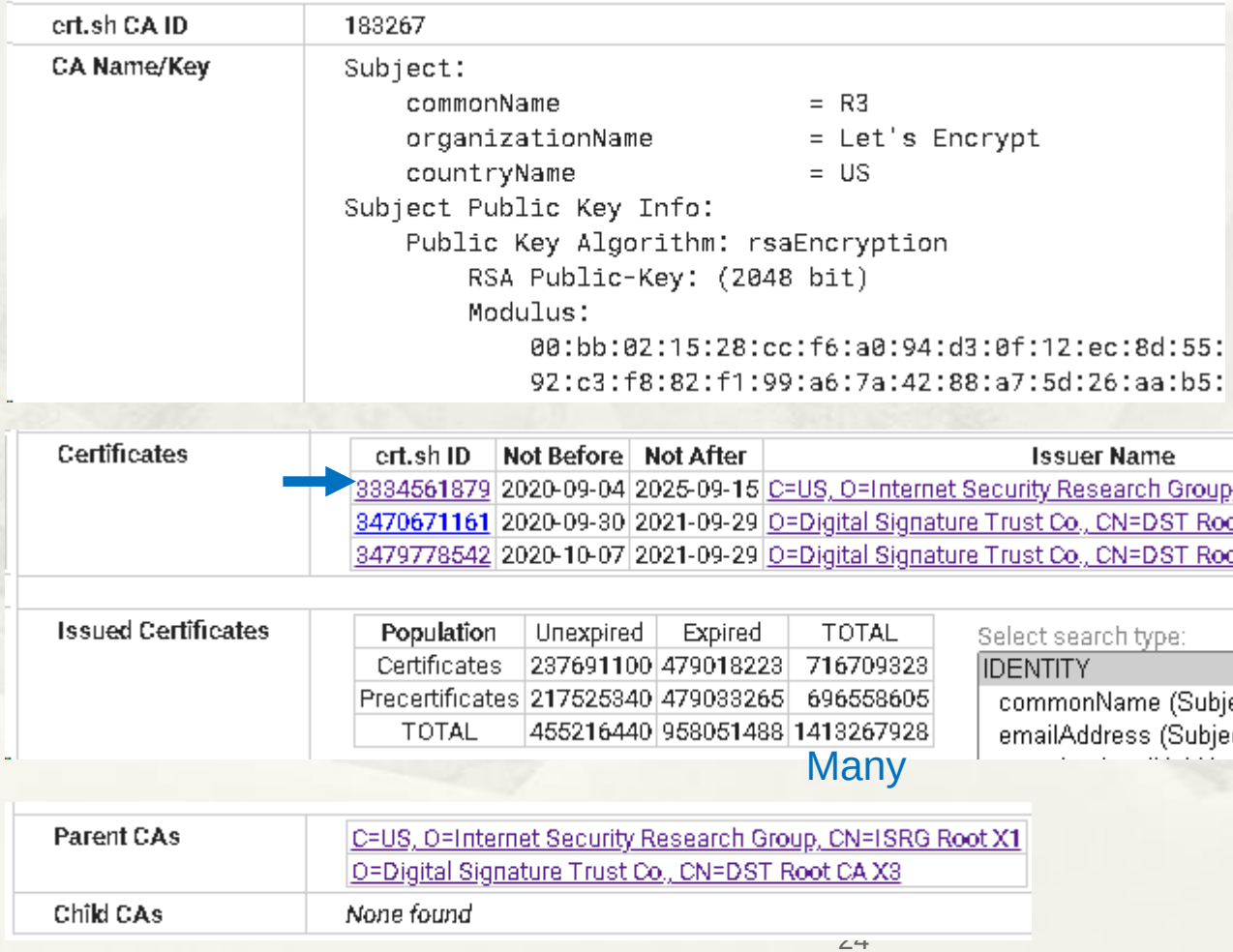
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:34:d3:01:86:14:a3:22:e0:a4:bb:61:a4:ab:dc:c3:bc:a3
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 183267)
            commonName               = R3
            organizationName         = Let's Encrypt
            countryName              = US
        Validity
            Not Before: Oct  8 01:50:56 2021 GMT
            Not After : Jan  6 01:50:55 2022 GMT
        Subject:
            commonName               = www.tp1rc.edu.tw
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b6:18:39:2b:53:32:fd:e9:b8:66:3d:4b:71:82:
                    76:cd:55:b8:a5:4e:87:d4:f8:ff:19:d0:77:a8:16:
```

Signed by Intermediate CA

效期 3個月

Intermediate CA
CN=R3 O=Let's Encrypt

* https://crt.sh/?caid=183267



crt.sh CA ID	183267
CA Name/Key	Subject: commonName = R3 organizationName = Let's Encrypt countryName = US Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public-Key: (2048 bit) Modulus: 00:bb:02:15:28:cc:f6:a0:94:d3:0f:12:ec:8d:55: 92:c3:f8:82:f1:99:a6:7a:42:88:a7:5d:26:aa:b5:

Certificates	crt.sh ID	Not Before	Not After	Issuer Name
	3334561879	2020-09-04	2025-09-15	C=US, O=Internet Security Research Group, CN=ISRG Root X1
	3470671161	2020-09-30	2021-09-29	O=Digital Signature Trust Co., CN=DST Root CA X3
	3479778542	2020-10-07	2021-09-29	O=Digital Signature Trust Co., CN=DST Root CA X3

Signed by Root
Signed by Root
Signed by Root

Issued Certificates	Population	Unexpired	Expired	TOTAL
	Certificates	237691100	479018223	716709323
	Precertificates	217525340	479033265	696558605
	TOTAL	455216440	958051488	1413267928

Select search type:
IDENTITY
commonName (Subject)
emailAddress (Subject)

Many

Parent CAs	C=US, O=Internet Security Research Group, CN=ISRG Root X1 O=Digital Signature Trust Co., CN=DST Root CA X3
Child CAs	*None found*

Intermediate Certificate CN=R3

* https://crt.sh/?id=3334561879

Certificate: → Intermediate Certificate Download (PEM format)

```
    Data:
        Version: 3 (0x2)
        Serial Number:
            91:2b:08:4a:cf:0c:18:a7:53:f6:d6:2e:25:a7:5f:5a
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 7394)
            commonName                = ISRG Root X1
            organizationName          = Internet Security Research Group
            countryName               = US
        Validity
            Not Before: Sep  4 00:00:00 2020 GMT
            Not After : Sep 15 16:00:00 2025 GMT
        Subject: (CA ID: 183267)
            commonName                = R3
            organizationName          = Let's Encrypt
            countryName               = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:bb:02:15:28:cc:f6:a0:94:d3:0f:12:ec:8d:55:
                    92:c3:f8:82:f1:99:a6:7a:42:88:a7:5d:26:aa:b5:
```

Signed by Root CA

効期 5年

Root CA
CN=ISRG Root X1 (1/2)

* https://crt.sh/?caid=7394

crt.sh CA ID	7394
CA Name/Key	Subject: commonName = ISRG Root X1 organizationName = Internet Security Research Group countryName = US Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public-Key: (4096 bit) Modulus: 00:ad:e8:24:73:f4:14:37:f3:9b:9e:2b:57:28:1c: 87:be:dc:b7:df:38:90:8c:6e:3c:e6:57:a0:78:f7:

CA 有效日期

Certificates	crt.sh ID	Not Before	Not After	Issuer Name
	9314791	2015-06-04	2035-06-04	C=US, O=Internet Security Research Group, CN=ISRG Root X1
	3958242236	2021-01-20	2024-09-30	O=Digital Signature Trust Co., CN=DST Root CA X3

Self-signed
Cross-signed

Issued Certificates	Population	Unexpired	Expired	TOTAL
	Certificates	5	5	10
	Precertificates	0	0	0
	TOTAL	5	5	10

Select search type:
IDENTITY
commonName (Subject)
emailAddress (Subject)

Enter sea
(% = All ce

Very few

Root CA
CN=ISRG Root X1 (2/2)

Trust

Purpose	Context (Version) Shortest Path Disabled From NotBefore Until									
	360 Browser (2021-08-05)	Apple (macOS 11.2)	Microsoft (2021-09-10)	Mozilla (2021-09-17)	Chrome (2020-05-15)	Android (2021-10-06)	Java (16.0.1)	Adobe CDS	Adobe AATL (2021-09-22)	Adobe EUTL (2021-10-01)
Server Authentication	No	Valid [1]	Valid [1]	Valid [1]	Defer to OS	Valid [1]	Valid [1]	n/a	n/a	n/a
Client Authentication	n/a	n/a	Valid [1]	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Secure Email	n/a	Valid [1]	Expired [2]	No	n/a	n/a	n/a	n/a	No	No
Code Signing	n/a	Valid [1]	No	n/a	n/a	n/a	Valid [1]	n/a	No	No
Kernel Mode Code Signing	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Time Stamping	n/a	Valid [1]	Expired [2]	n/a	n/a	n/a	n/a	n/a	n/a	n/a
OCSP Signing	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Document Signing	n/a	n/a	Expired [2]	n/a	n/a	n/a	n/a	n/a	No	No
Encrypting File System	n/a	n/a	Expired [2]	n/a	n/a	n/a	n/a	n/a	n/a	n/a
IP security end system	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a
IP security IKE intermediate	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a
IP security tunnel termination	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a
IP security user	n/a	Valid [1]	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Adobe Authentic Document	n/a	n/a	n/a	n/a	n/a	n/a	n/a	No	No	No

Parent CAs

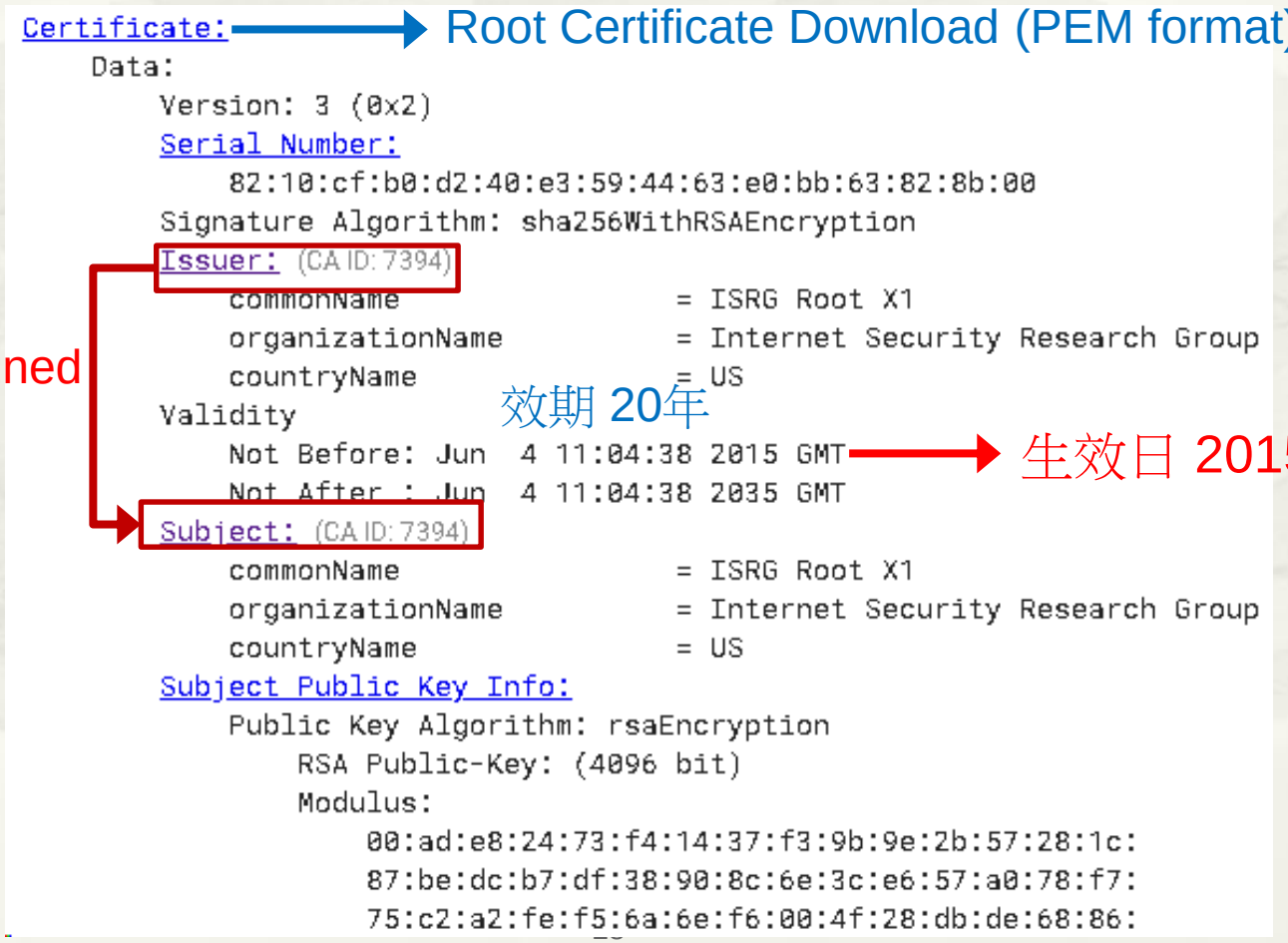
O=Digital Signature Trust Co., CN=DST Root CA X3

Child CAs

C=US, O=Internet Security Research Group, CN=ISRG Root X2
C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X1
C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X2
C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X4
C=US, O=Let's Encrypt, CN=R3
C=US, O=Let's Encrypt, CN=R4

Root Certificate
CN=ISRG Root X1

* https://crt.sh/?id=9314791



Root Certificate
CN=ISRG Root X1

* https://crt.sh/?id=3958242236

Cross-signed

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            40:01:77:21:37:d4:e9:42:b8:ee:76:aa:3c:64:0a:b7
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 276)
            commonName                = DST Root CA X3
            organizationName          = Digital Signature Trust Co.
        Validity
            Not Before: Jan 20 19:14:03 2021 GMT
            Not After : Sep 30 18:14:03 2024 GMT
        Subject: (CA ID: 7394)
            commonName                = ISRG Root X1
            organizationName          = Internet Security Research Group
            countryName               = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:ad:e8:24:73:f4:14:37:f3:9b:9e:2b:57:28:1c:
                    87:be:dc:b7:df:38:90:8c:6e:3c:e6:57:a0:78:f7:
```

效期 3.5年

Root CA
CN= DST Root CA X3

* https://crt.sh/?caid=276

crt.sh CA ID	276
CA Name/Key	Subject: commonName = DST Root CA X3 organizationName = Digital Signature Trust Co. Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public-Key: (2048 bit) Modulus: 00:df:af:e9:97:50:08:83:57:b4:cc:62:65:f6:90: 82:ec:c7:d3:2c:6b:30:ca:5b:ec:d9:c3:7d:c7:40:

CA 有效日期

Certificates	crt.sh ID	Not Before	Not After	Issuer Name
	8986898	2000-09-30	2008-01-21	C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co., OU=DSTCA X1, CN=DST RootCA X1, emailAddress=ca@digsigtrust.com
	8376050	2004-09-08	2008-11-28	C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co., OU=DSTCA X1, CN=DST RootCA X1, emailAddress=ca@digsigtrust.com
	12729327	2004-09-08	2008-11-27	C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co., OU=DSTCA X1, CN=DST RootCA X1, emailAddress=ca@digsigtrust.com
	8395	2000-09-30	2021-09-30	O=Digital Signature Trust Co., CN=DST Root CA X3

全部已過期

* CA 已過期，所簽發之 Certificate 有效 or 無效？

Root Certificate
CN=DST Root CA X3

* https://crt.sh/?id=8395

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            44:af:b0:80:d6:a3:27:ba:89:30:39:86:2e:f8:40:6b
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: (CA ID: 276)
            commonName                = DST Root CA X3
            organizationName          = Digital Signature Trust Co.
        Validity (Expired)
            Not Before: Sep 30 21:12:19 2000 GMT
            Not After : Sep 30 14:01:15 2021 GMT
        Subject: (CA ID: 276)
            commonName                = DST Root CA X3
            organizationName          = Digital Signature Trust Co.
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:df:af:e9:97:50:08:83:57:b4:cc:62:65:f6:90:
                    82:ec:c7:d3:2c:6b:30:ca:5b:ec:d9:c3:7d:c7:40:
```

效期 21年

到期日 2021/09/30

Certificate Chain Problems

Certificate Chain Problems

- All operating systems contain a set of default trusted root certificates.
- But Certificate Authorities usually don't use their root certificate to sign customer certificates.
- They use so called intermediate certificates instead, because these can be rotated more frequently(有效日期較短).
- If not all intermediate certificates are installed on your server,
  - some clients(Old browsers, curl, LineAPI) will think it’s an insecure connection.
  - 新版瀏覽器(Chrome. Firefox)都很 “聰明”，會自動修正或補齊 web server 提供的錯誤憑證鏈，甚至 web server 不提供中繼及根憑證都不會有問題.
- Best Practice
  - Server should always send a complete trust chain. The trust chain contains your certificate concatenated with all intermediate certificates.

Certificate Chain Check

- Online Service
  - https://www.digicert.com/help/
  - https://www.ssllabs.com/ssltest/analyze.html
  - https://check.twnic.tw/

Certificate Chain Check

- Client Program (需提供正確 Intermediate Certificate 才能連線)
  - 使用舊版 Browser, wget
  - curl -v https://www.ntub.edu.tw
  - curl -v https://incomplete-chain.badssl.com

```
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: /etc/ssl/certs
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS alert, unknown CA (560):
* SSL certificate problem: unable to get local issuer certificate
* Closing connection 0
curl: (60) SSL certificate problem: unable to get local issuer certificate
More details here: https://curl.haxx.se/docs/sslcerts.html
```

發生錯誤, 無法連線

Certificate Chain Check
人工自行檢查

* openssl s_client -connect www.ntu.edu.tw:443 -servername www.ntu.edu.tw

```
Certificate chain
 0 s:C = TW, ST = Taiwan, L = Taipei, O = National Taiwan University, OU = Computer and Information Networking Center, CN = *.ntu.edu.tw
   i:C = TW, O = TAIWAN-CA, OU = Secure SSL Sub-CA, CN = TWCA Secure SSL Certification Authority
 1 s:C = TW, O = TAIWAN-CA, OU = Secure SSL Sub-CA, CN = TWCA Secure SSL Certification Authority
   i:C = TW, O = TAIWAN-CA, OU = Root CA, CN = TWCA Global Root CA
 2 s:C = TW, O = TAIWAN-CA, OU = Root CA, CN = TWCA Global Root CA
   i:C = TW, O = TAIWAN-CA, OU = Root CA, CN = TWCA Root Certification Authority
 3 s:C = TW, O = TAIWAN-CA, OU = Root CA, CN = TWCA Root Certification Authority
   i:C = TW, O = TAIWAN-CA, OU = Root CA, CN = TWCA Root Certification Authority
```

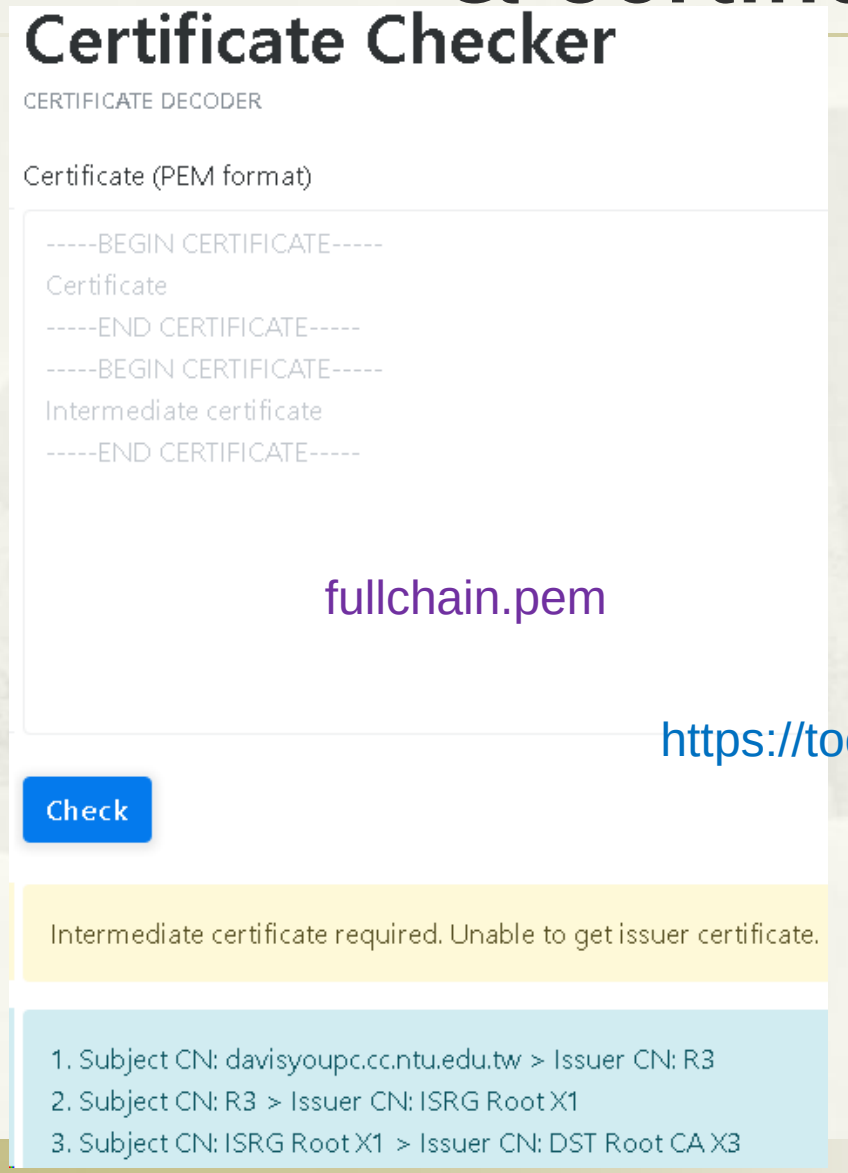
正確

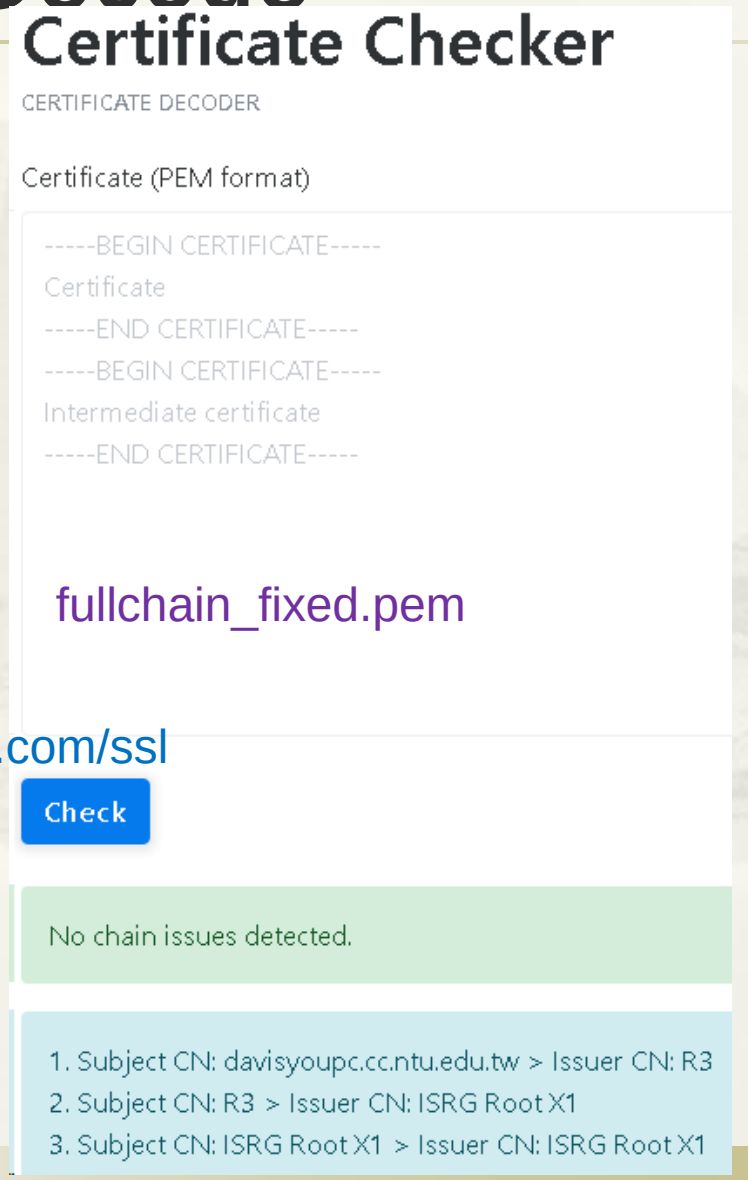
* openssl s_client -connect www.ntub.edu.tw:443 -servername www.ntub.edu.tw

```
depth=0 CN = *.ntub.edu.tw
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = *.ntub.edu.tw
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:CN = *.ntub.edu.tw
   i:C = US, O = DigiCert Inc, CN = RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1
 1 s:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
   i:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
 2 s:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = RapidSSL TLS RSA CA G1
   i:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
```

異常

Certificate Chain Check & Certificate Decode





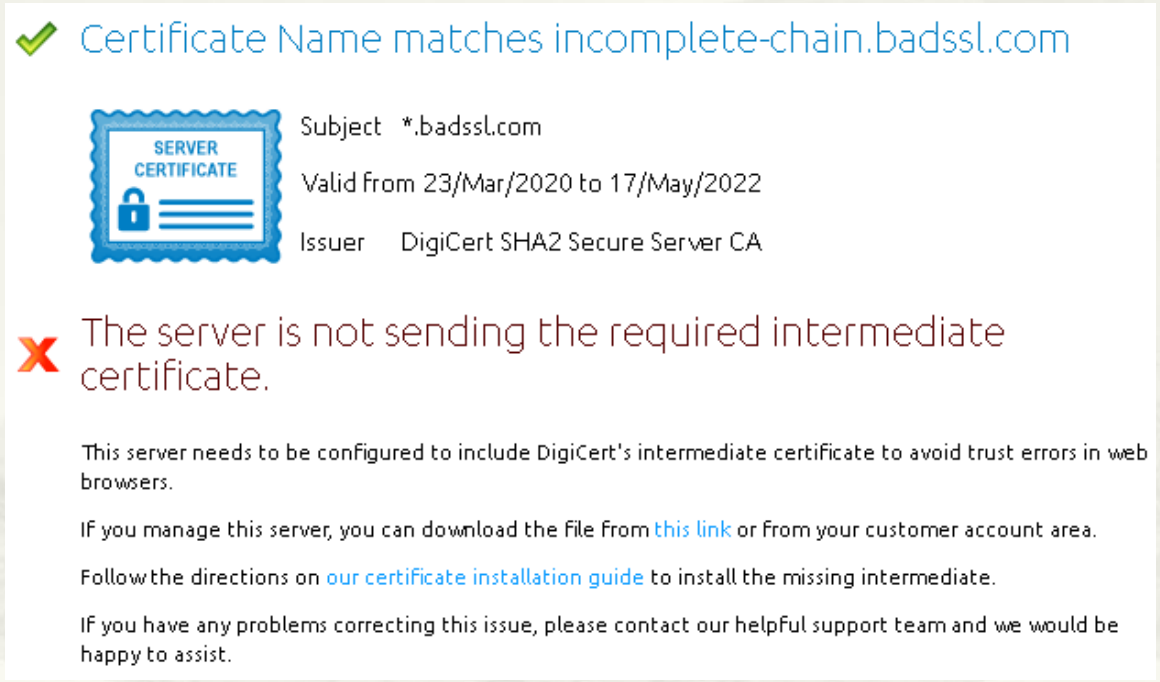
https://tools.keycdn.com/ssl

案例: 未提供 Intermediate Certificate

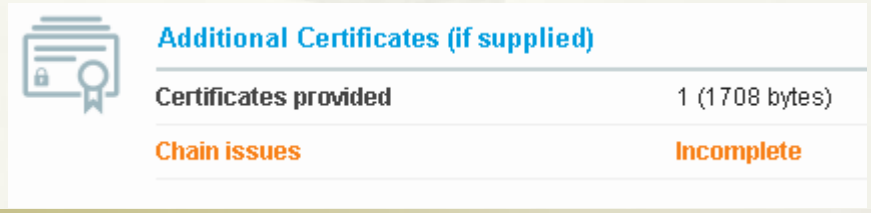
僅提供 Server Certificate

未提供 Intermediate Certificate incomplete-chain.badssl.com

* https://www.digicert.com/help

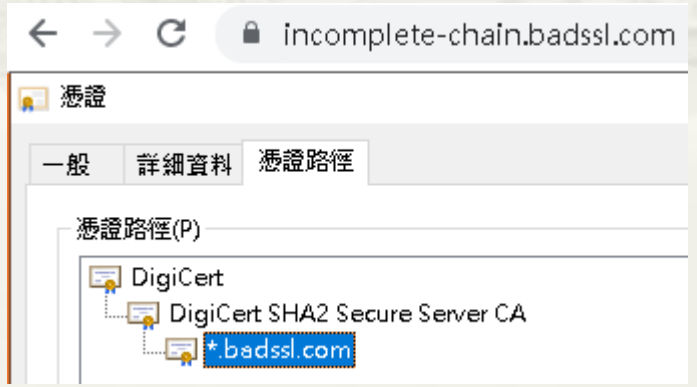


* https://www.ssllabs.com/ssltest/analyze.html



* https://check.twnic.tw

* Chrome 會自行修正

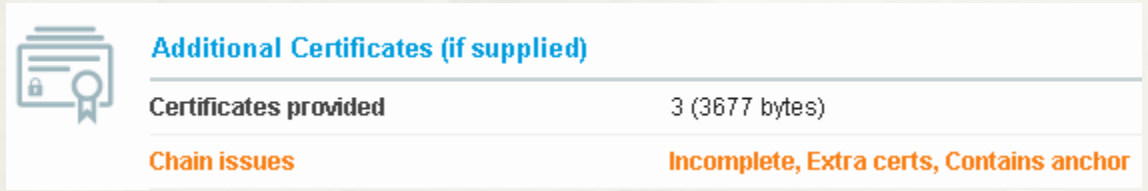


案例: 提供錯誤 **Intermediate Certificate**

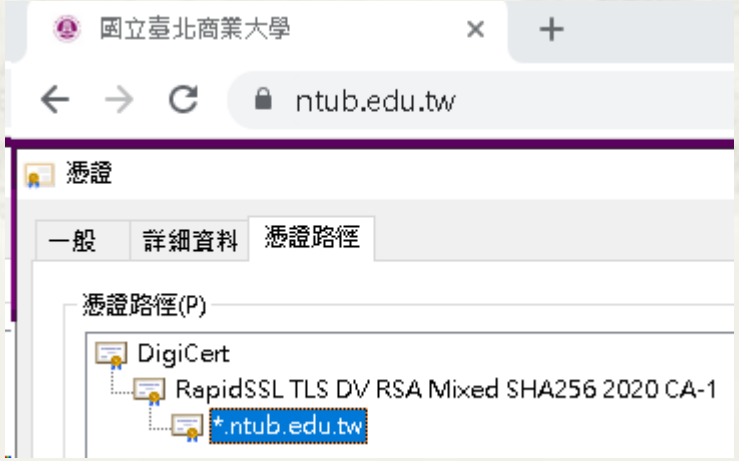
提供錯誤 Intermediate Certificate www.ntub.edu.tw

* https://www.digicert.com/help/

* https://www.ssllabs.com/ssltest/analyze.html



* Chrome 自行修正



案例: Root Certificate 過期

根憑證到期日
≈ SSL 數位憑證審判日

* DST Root CA X3 根憑證過期

* 2020/05/30，串流製造商Roku、支付業者Stripe與Spreedly、雲端儲存服務SugarSync等數十種服務，都在同一個時間停擺
* https://www.ithome.com.tw/news/138197

SSL 數位憑證審判日

* https://letsencrypt.org/docs/certificate-compatibility/

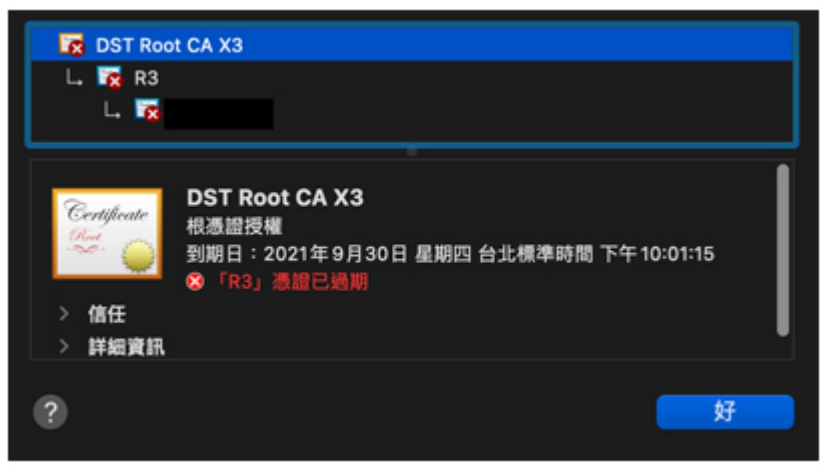
Platforms that trust DST Root CA X3 but not ISRG Root X1

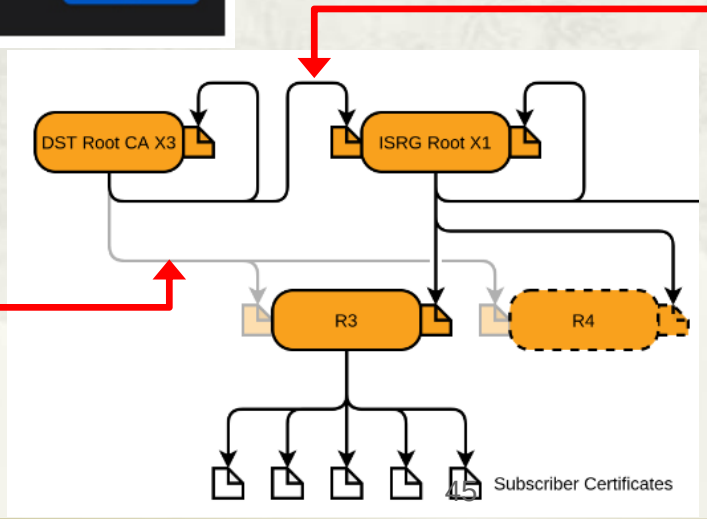
These platforms would have worked up to September 2021 but will no longer validate Let's Encrypt certificates.

- macOS < 10.12.1
- iOS < 10
- Mozilla Firefox < 50
- Ubuntu >= intrepid / 8.10
- Debian >= squeeze / 6 and < jessie /8
- Java 8 >= 8u101 and < 8u141
- Java 7 >= 7u111 and < 7u151
- NSS >= v3.11.9 and < 3.26
- Amazon FireOS (Silk Browser) (version range unknown)
- Cyanogen > v10 (version that added ISRG Root X1 unknown)
- Jolla Sailfish OS > v1.1.2.16 (version that added ISRG Root X1 unknown)
- Kindle > v3.4.1 (version that added ISRG Root X1 unknown)
- Blackberry >= 10.3.3 (version that added ISRG Root X1 unknown)
- PS4 game console with firmware >= 5.00 (version that added ISRG Root X1 unknown)

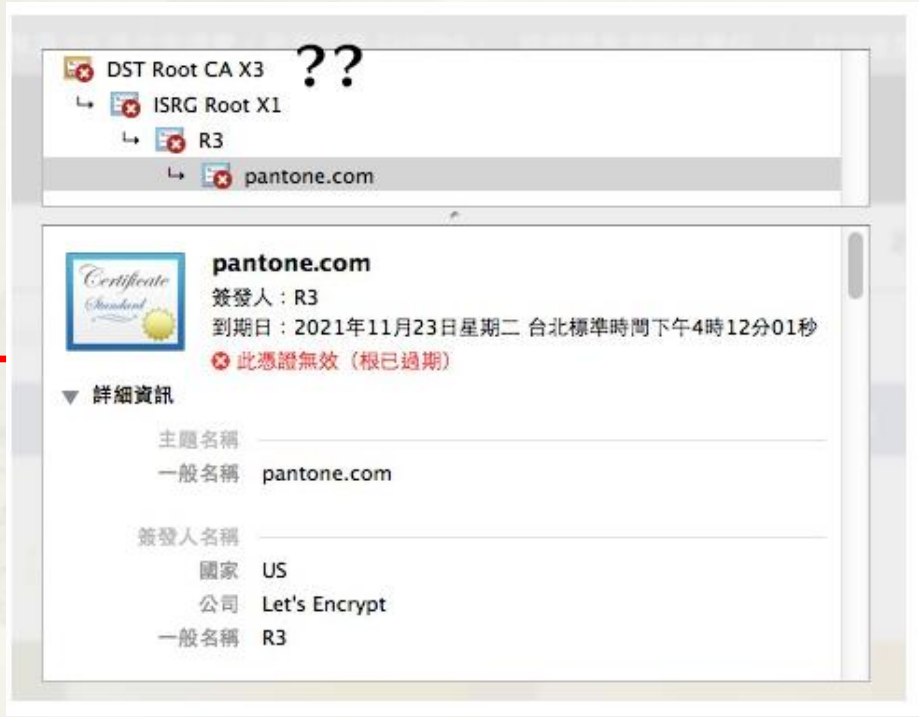
SSL 數位憑證審判日

* 使用已過期之 Certificate Chain



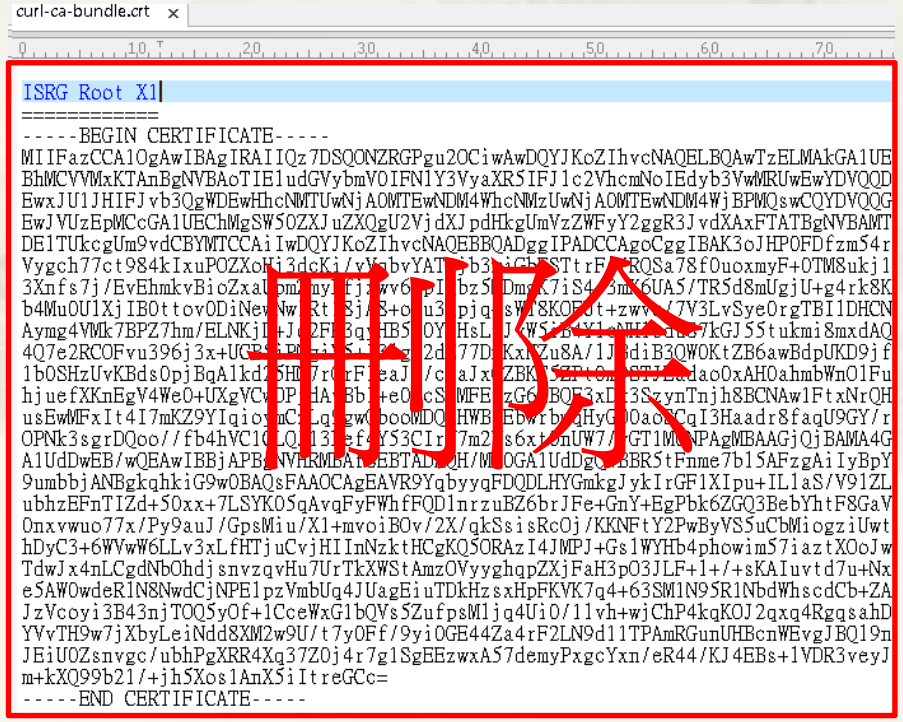


* 系統太舊(早於 2015年)，尚未包含 ISRG Root X1 根憑證



使用 curl 模擬
無 ISRG Root X1 根憑證

- curl for Windows
  https://curl.se/windows/
- Edit curl-ca-bundle.crt



- curl -v https://letsencrypt.org

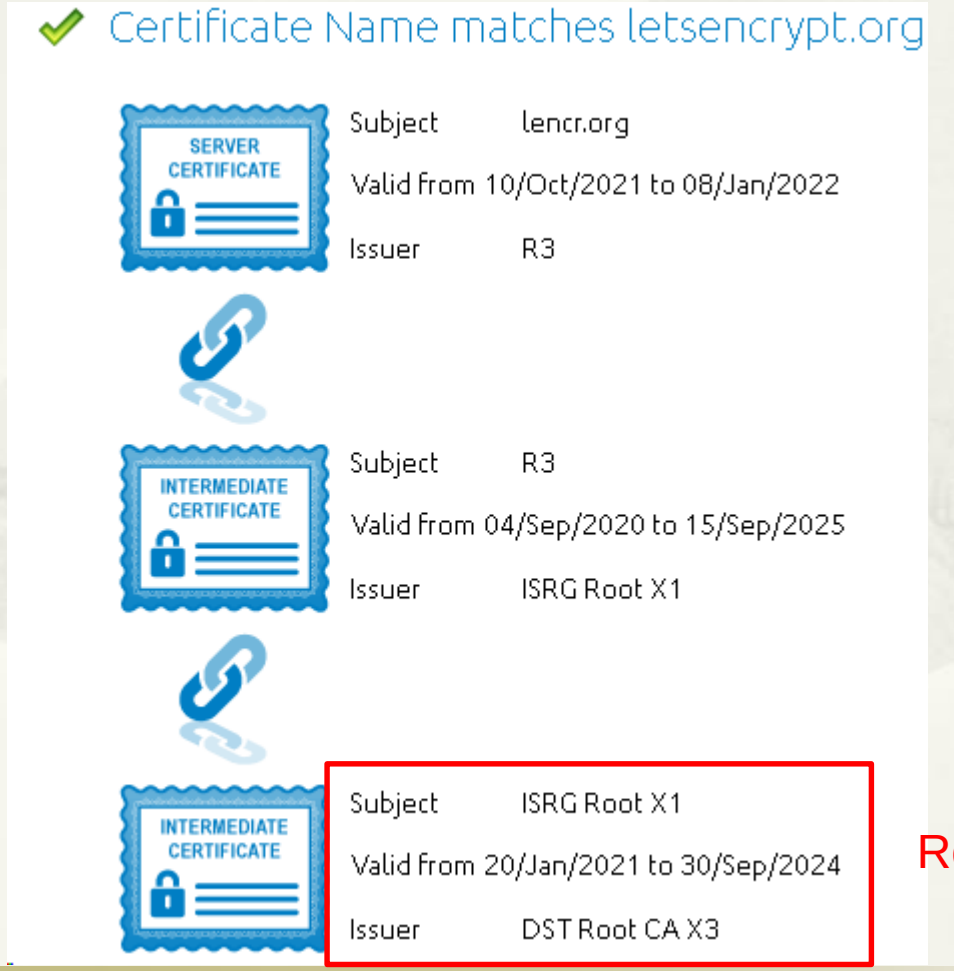
```
D:\curl-7.79.1-win64-mingw\bin>curl -v https://letsencrypt.org
*   Trying 3.0.239.142:443...
* Connected to letsencrypt.org (3.0.239.142) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
*  CAfile: D:\curl-7.79.1-win64-mingw\bin\curl-ca-bundle.crt
* TLSv1.0 (OUT), TLS header, Certificate Status (22):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS header, Certificate Status (22):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS header, Finished (20):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS header, Unknown (21):
* TLSv1.3 (OUT), TLS alert, unknown CA (560):
* SSL certificate problem: unable to get local issuer certificate
* Closing connection 0
curl: (60) SSL certificate problem: unable to get local issuer certificate
More details here: https://curl.se/docs/sslcerts.html
```

發生錯誤, 無法連線

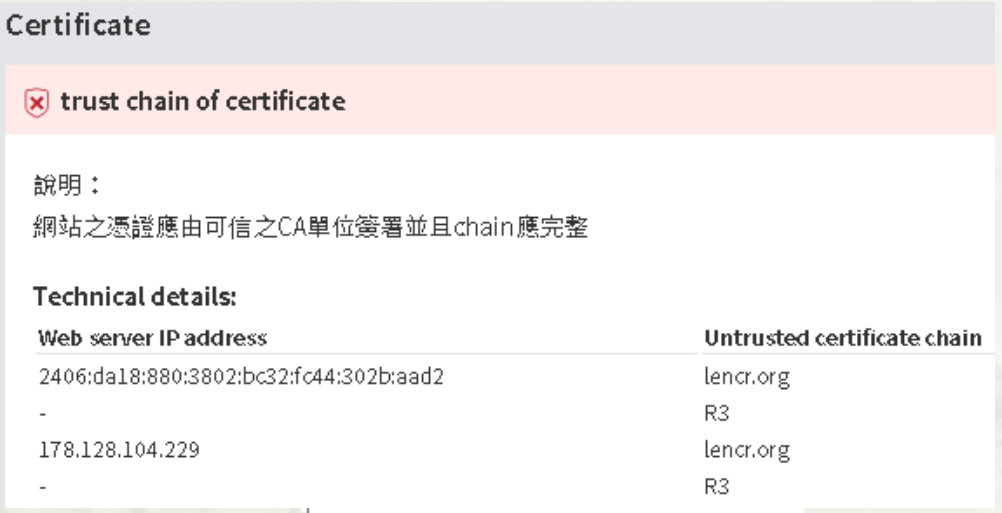
案例: Root Certificate Cross-signed With Expired CA

letsencrypt.org

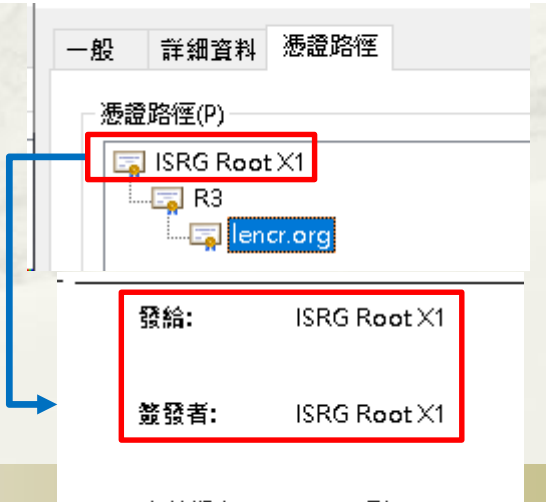
* https://www.digicert.com/help



* https://check.twnic.tw/



* Chrome



Root Certificate 不相同

Root Certificate Cross-signed With Expired CA

* 所有使用 Let's Encrypt 憑證之網站皆有相同問題
* TANet NOC
  * https://noc.tanet.edu.tw/
* 政大區網
  * https://tp2rc.tanet.edu.tw/
* 交大區網
  * www.hcrc.edu.tw
* 台大區網 (已修正)
  * www.tp1rc.edu.tw

How to Fix Certificate Chain Problems

Should Certificate Chain Need Include Root Certificate ?

- You do not need to include the root certificate in the certificate chain.
- Since clients already have the root certificate in their trust stores.
- Including the root is inefficient since it increases the size of the SSL handshake and browsers will simply ignore it.

Generate Intermediate Certificate Online

* https://whatsmychaincert.com/
  * Certificate (PEM format)
  * Online use hostname
* https://tools.keycdn.com/certificate-chain
  * Certificate (PEM format)
* https://certificatechain.io/
  * Certificate (PEM format)

Certificate Files

- **privkey.pem**
  - Private key for the certificate.
- **cert.pem**
  - Server certificate only.
- **chain.pem**
  - All certificates that need to be served by the browser excluding server certificate
  - Intermediate + Root certificate(optional)
- **fullchain.pem**
  - All certificates, including server certificate.
  - This is concatenation of chain.pem and cert.pem.
  - Server + Intermediate + Root certificate(optional)

SSL Config for Linux

- SSLCertificateKeyFile /etc/letsencrypt/live/www.tp1rc.edu.tw/privkey.pem
- 以下設定二擇一
  - SSLCertificateFile /etc/letsencrypt/live/www.tp1rc.edu.tw/fullchain.pem
  - OR
  - SSLCertificateFile /etc/letsencrypt/live/www.tp1rc.edu.tw/cert.pem
  - SSLCertificateChainFile /etc/letsencrypt/live/www.tp1rc.edu.tw/chain.pem

簡報完畢
謝謝