HTTPS 憑證簽署架構
CA & Certificate

臺灣大學計資中心

網路組

游子興

大綱

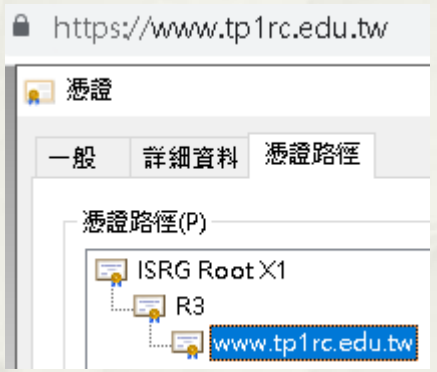
* Certificate Authority & Certificate
* Certificate Format
* Root Certificate 根憑證
* Certificate Type
* 其他

Certificate Authority & Certificate

Certificate Chain Example

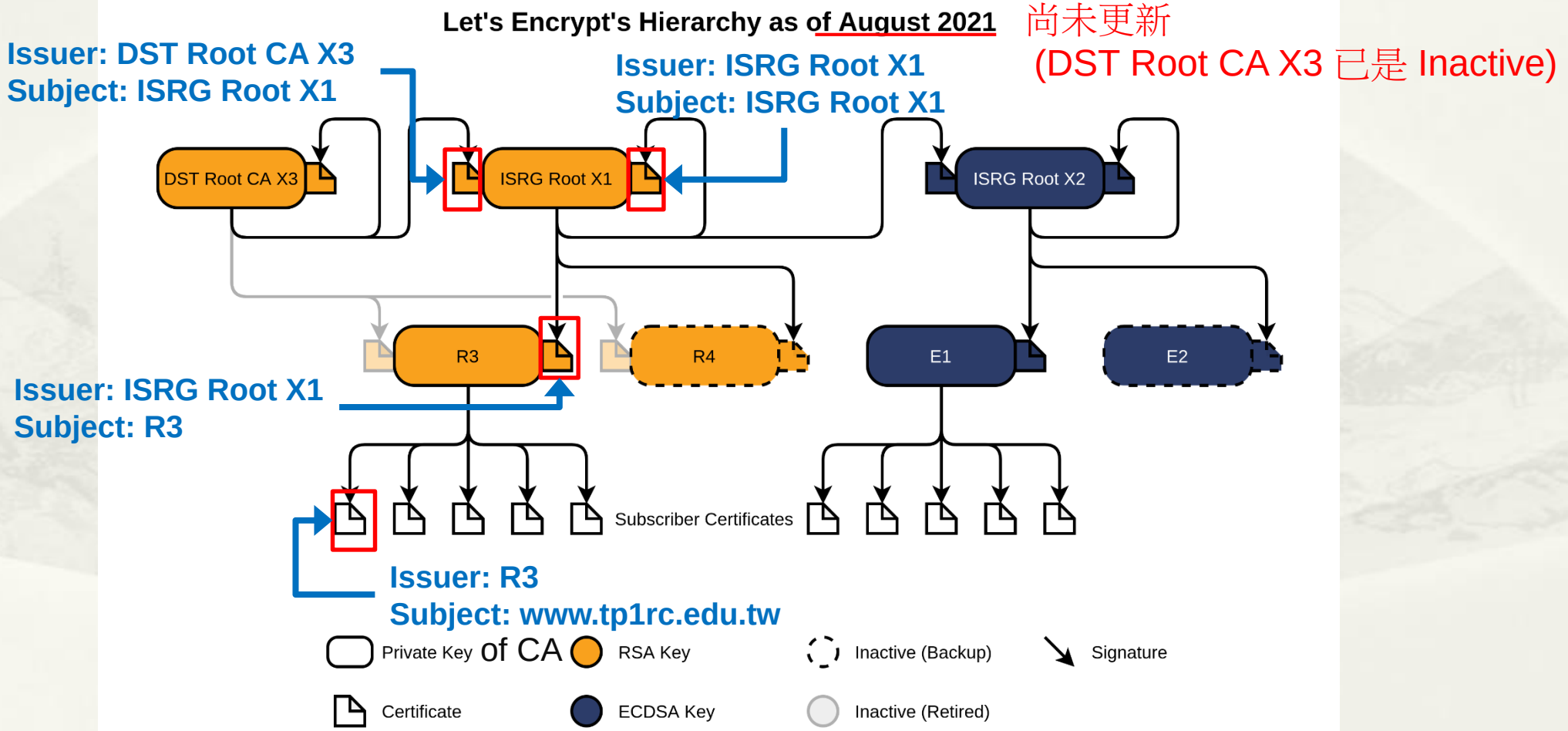
* www.ntu.edu.tw

* www.tp1rc.edu.tw



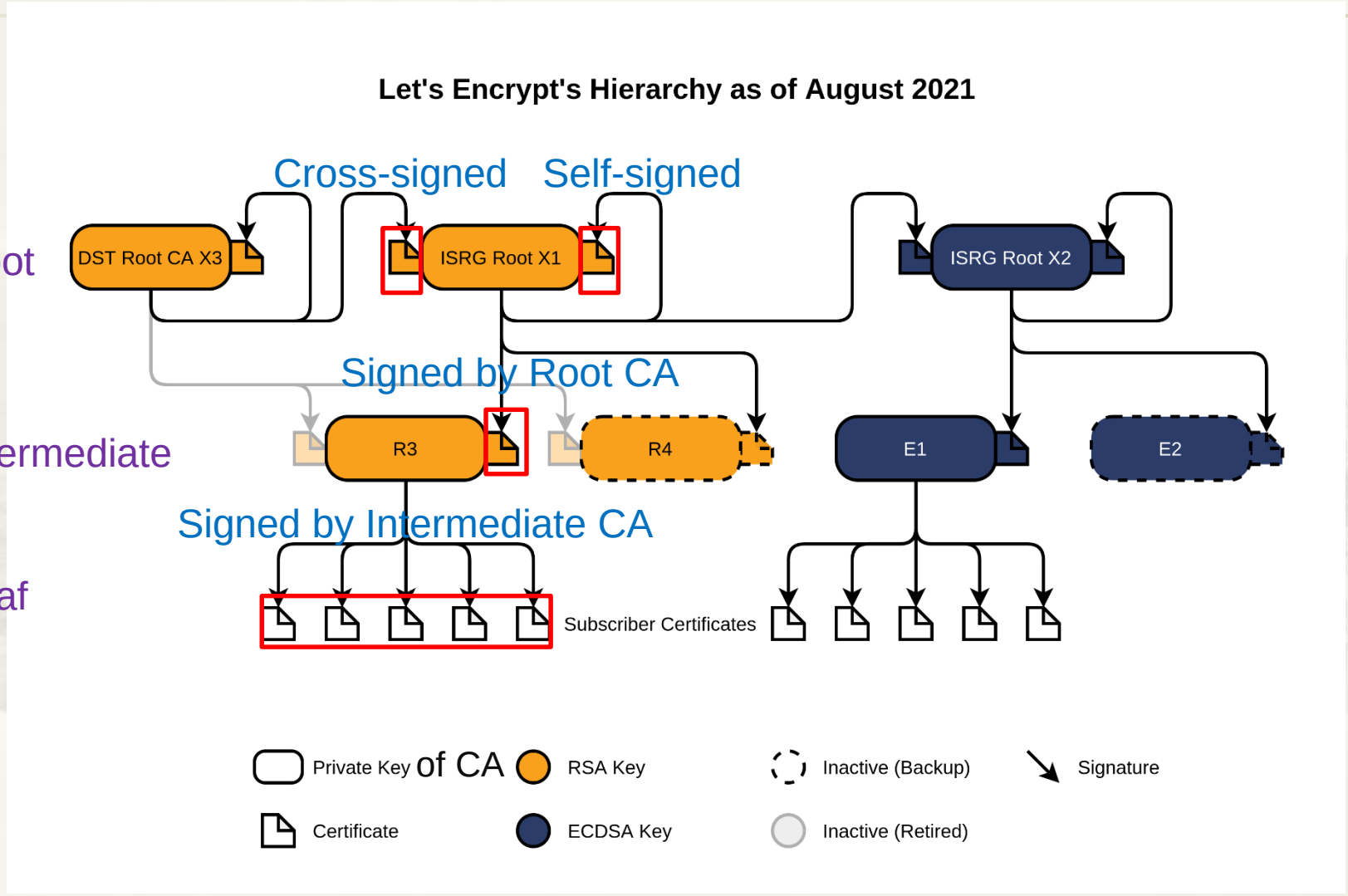
Let's Encrypt Chain of Trust

https://letsencrypt.org/certificates/



尚未更新
(DST Root CA X3 已是 Inactive)

Let's Encrypt Chain of Trust



Certificate Authority(CA)
憑證簽證機關

- Root CA
  - 用途: Issue Certificate to Root/Intermediate CA
- Intermediate CA
  - 用途: 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: 發出之憑證
  - Trust: Support OS/Browser
  - Parent CAs：based on Certificates
  - Child CAs: based on Issued Certificates

Certificate : CA 簽發之憑證

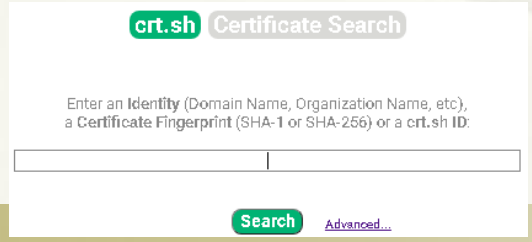
- Root Certificate 根憑證: Used by Root CA
  - Self-signed (效期: 20 ~25年)
- Intermediate Certificate 中繼憑證: Used by Intermediate CA
  - Signed by Root CA (效期:5年)
- Leaf Certificate: Used by Web Server
  - Signed by Intermediate CA (效期: 1~2年)
- ※ Cross-signed: Signed by the same Level of CA (Root/Intermediate Certificate)
- 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: X509 v3 Extensions

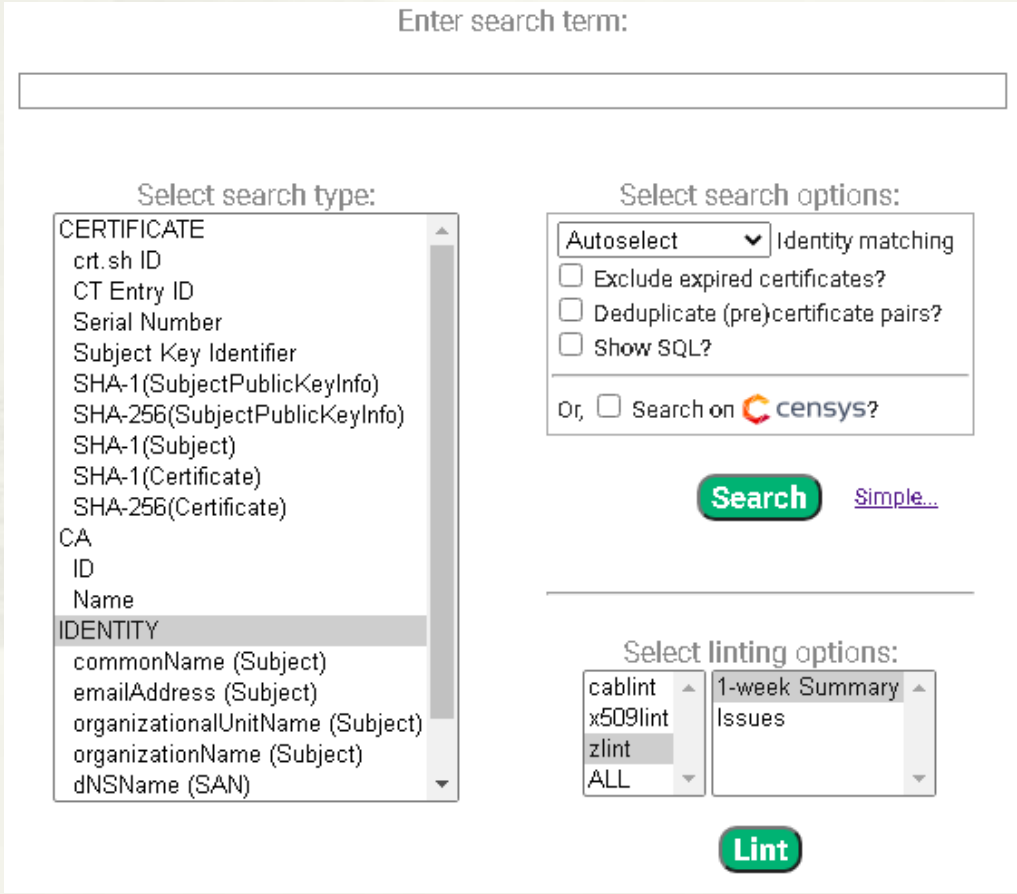
* X509v3 Extended Key Usage
  * TLS Web Server Authentication
  * TLS Web Client Authentication
* X509v3 Basic Constraints: critical
  * CA:FALSE → Leaf Certificate (Used by Web Server)
  * CA:TRUE → Root/Intermediate Certificate (Used by CA)
* X509v3 Subject Alternative Name (SAN)
  * DNS:www.tp1rc.edu.tw
* X509v3 Certificate Policies
  * Policy: 2.23.140.1.2.1
  * Policy: 1.3.6.1.4.1.44947.1.1.1

Certificate Search Engine https://crt.sh

- 記錄分兩種
  - CA or Certificate
- commonName,
  - https://crt.sh/?CN=www.tp1rc.edu.tw
  - https://crt.sh/?CN=*.ntu.edu.tw
- Domain Name (Subject Alternative Name)
  - https://crt.sh/?dNSName=ee.ntu.edu.tw
    - 結尾是 ee.ntu.edu.tw
- 搜尋任意關鍵字 (Google Like Search)
  - 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

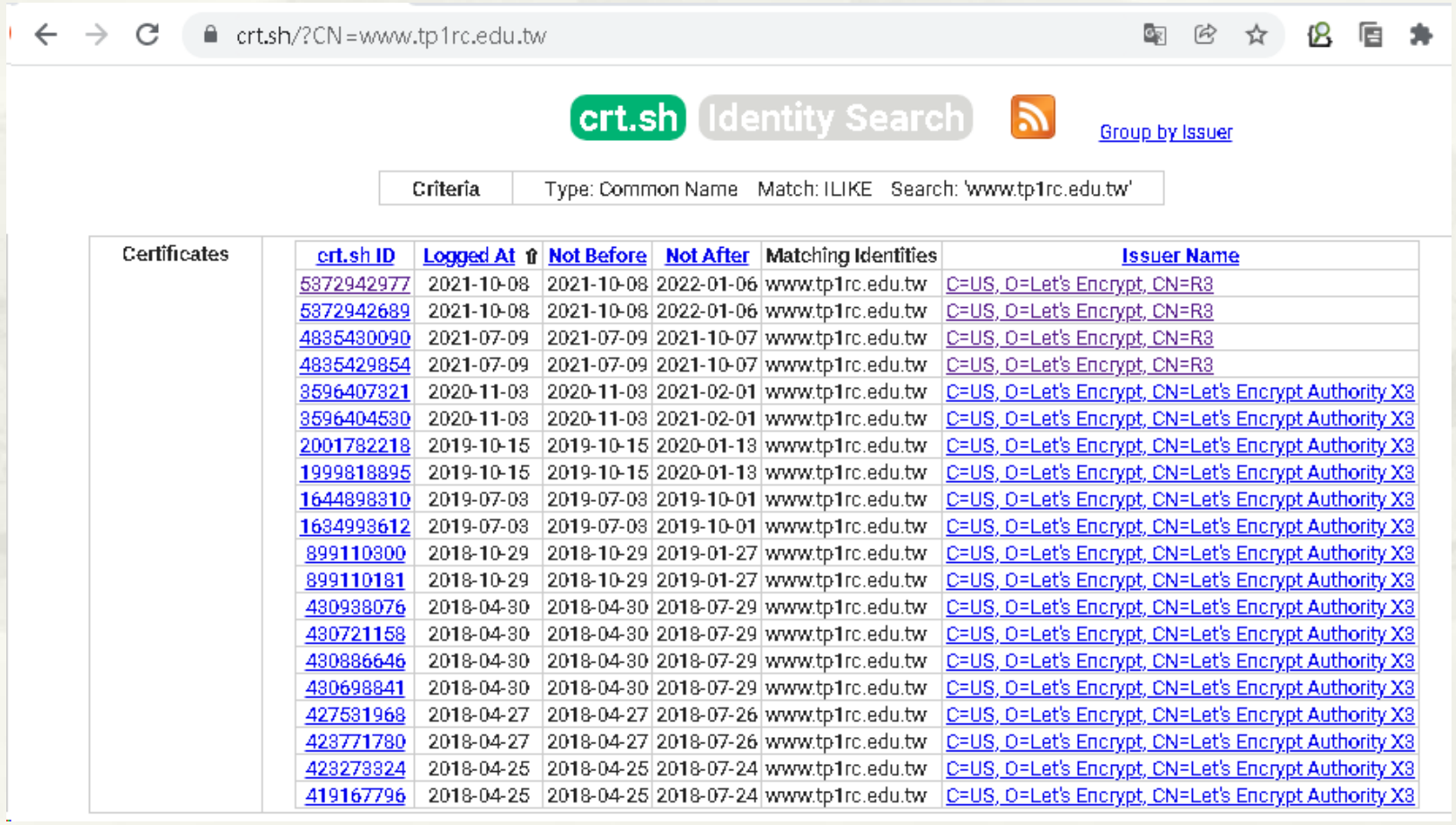


- Advanced Search



Server Certificate History

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



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

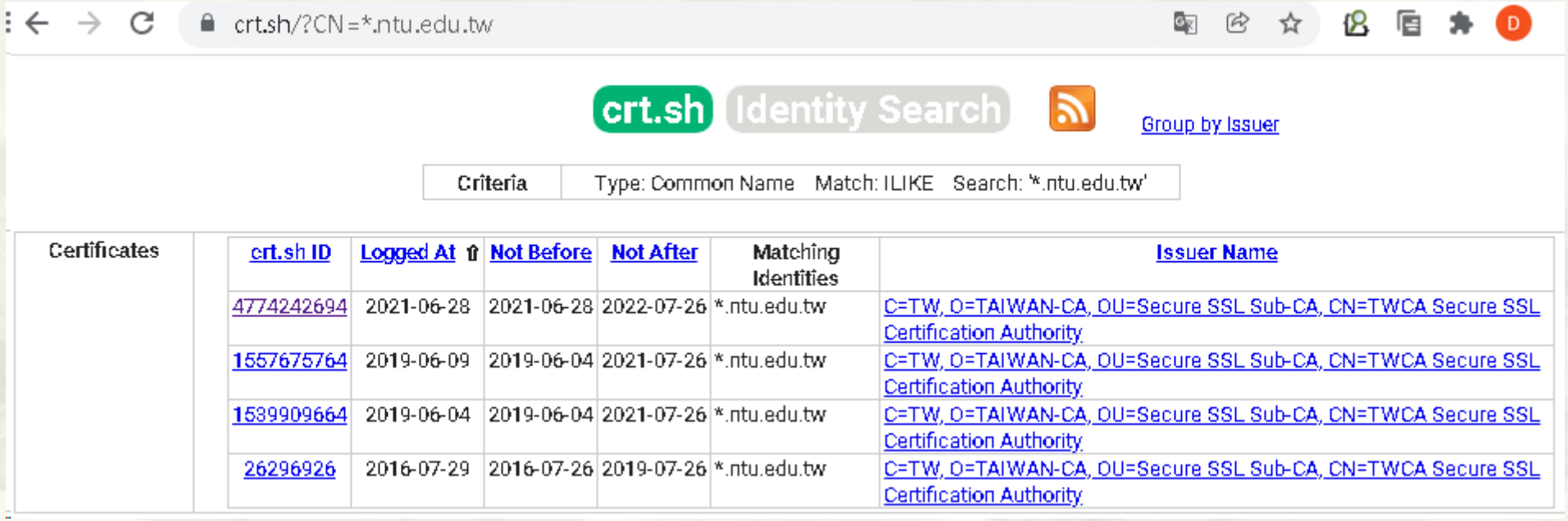
Select search type:
IDENTITY
commonName (Subject)
emailAddress (Subject)

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*

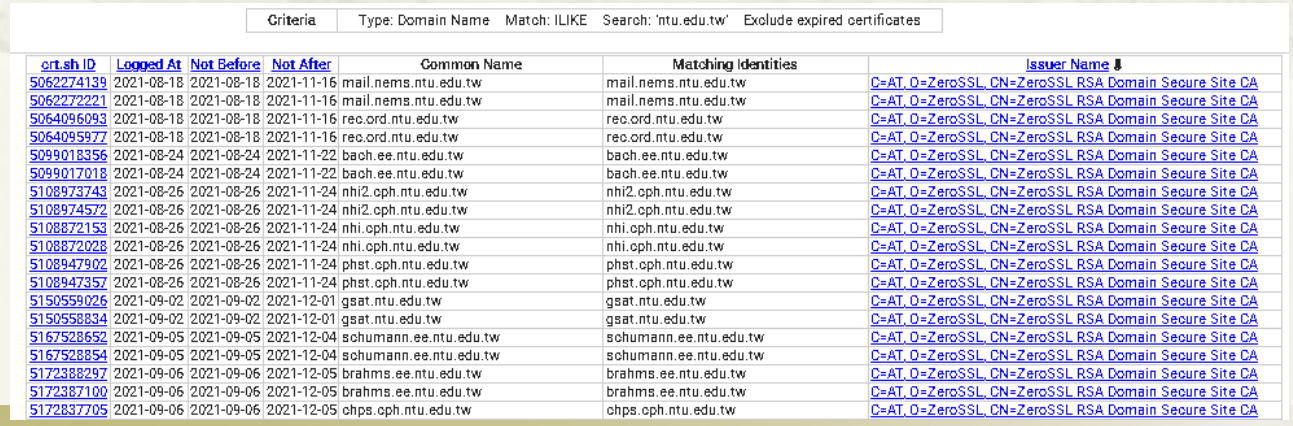
Server Certificate History

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



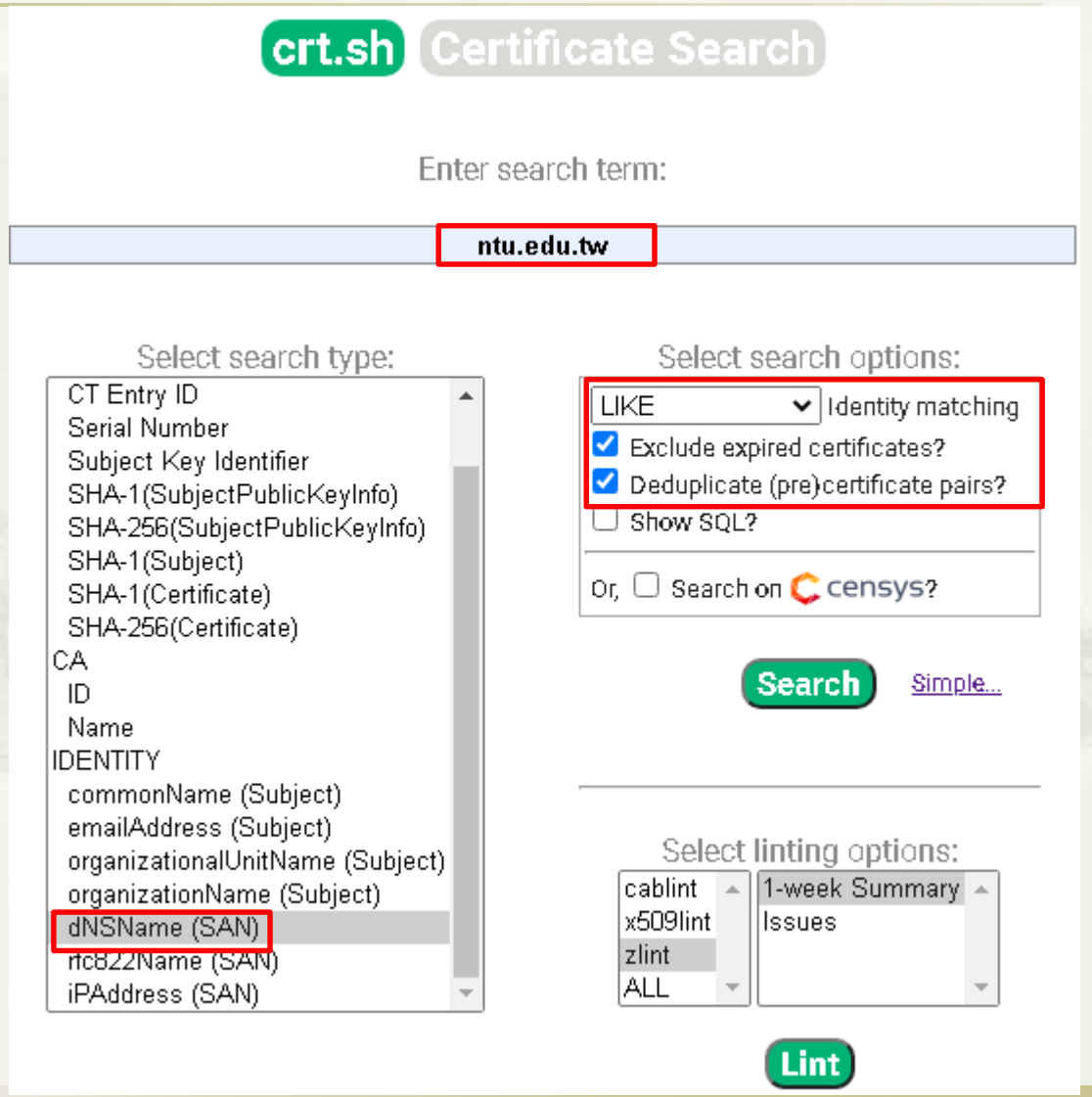
ntu.edu.tw 憑證統計

- https://crt.sh/?dNSName=ntu.edu.tw&exclude=expired&match=LIKE&deduplicate=Y
- Criteria
  - Type: Domain Name
  - Match: LIKE Search: 'ntu.edu.tw'
  - Exclude expired certificates
- 搜尋結果:



Criteria | Type: Domain Name | Match: ILIKE | Search: 'ntu.edu.tw' | Exclude expired certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
5062274139	2021-08-18	2021-08-18	2021-11-16	mail.nems.ntu.edu.tw	mail.nems.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5062272221	2021-08-18	2021-08-18	2021-11-16	mail.nems.ntu.edu.tw	mail.nems.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5064096093	2021-08-18	2021-08-18	2021-11-16	rec.ord.ntu.edu.tw	rec.ord.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5064095977	2021-08-18	2021-08-18	2021-11-16	rec.ord.ntu.edu.tw	rec.ord.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5099018356	2021-08-24	2021-08-24	2021-11-22	bach.ee.ntu.edu.tw	bach.ee.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5099017018	2021-08-24	2021-08-24	2021-11-22	bach.ee.ntu.edu.tw	bach.ee.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5108973743	2021-08-26	2021-08-26	2021-11-24	nhi2.cph.ntu.edu.tw	nhi2.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5108974572	2021-08-26	2021-08-26	2021-11-24	nhi2.cph.ntu.edu.tw	nhi2.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5108872153	2021-08-26	2021-08-26	2021-11-24	nhi.cph.ntu.edu.tw	nhi.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5108872028	2021-08-26	2021-08-26	2021-11-24	nhi.cph.ntu.edu.tw	nhi.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5108947902	2021-08-26	2021-08-26	2021-11-24	phst.cph.ntu.edu.tw	phst.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5108947357	2021-08-26	2021-08-26	2021-11-24	phst.cph.ntu.edu.tw	phst.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5150559026	2021-09-02	2021-09-02	2021-12-01	gsat.ntu.edu.tw	gsat.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5150558834	2021-09-02	2021-09-02	2021-12-01	gsat.ntu.edu.tw	gsat.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5167528652	2021-09-05	2021-09-05	2021-12-04	schumann.ee.ntu.edu.tw	schumann.ee.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5167528854	2021-09-05	2021-09-05	2021-12-04	schumann.ee.ntu.edu.tw	schumann.ee.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5172388297	2021-09-06	2021-09-06	2021-12-05	brahms.ee.ntu.edu.tw	brahms.ee.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5172387100	2021-09-06	2021-09-06	2021-12-05	brahms.ee.ntu.edu.tw	brahms.ee.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5172837705	2021-09-06	2021-09-06	2021-12-05	chps.cph.ntu.edu.tw	chps.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA



ntu.edu.tw 憑證統計

Issuer Name	計數	%
C=US, O=Let's Encrypt, CN=R3 (免費)	507	68
C=TW, O=TAIWAN-CA, OU=Secure SSL Sub-CA, CN=TWCA Secure SSL Certification Authority	114	15
C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"	44	6
C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA	26	3
C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA	19	3
C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA	13	2
C=TW, O="Chunghwa Telecom Co., Ltd.", OU=Public Certification Authority - G2	7	1
C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2	7	1
C=US, O=Google Trust Services LLC, CN=GTS CA 1D4	4	1
C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3	3	0
C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2	3	0
C=BE, O=GlobalSign nv-sa, CN=GlobalSign GCC R3 DV TLS CA 2020	1	0
C=TW, O=TAIWAN-CA, OU=Global EVSSL Sub-CA, CN=TWCA Global EVSSL Certification Authority	1	0
C=US, O=DigiCert Inc, CN=GeoTrust TLS DV RSA Mixed SHA256 2020 CA-1	1	0
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust EV RSA CA 2018	1	0
總計	751	100

ntu.edu.tw 有效憑證統計

* 統計結果

類別	總數	百分比 %
免費	507	68
付費	244	32

* 付費憑證價格: https://www.twca.com.tw/sslService

* .ntu.edu.tw 一年付費憑證費用

244 * 3780 = $922,320

(若使用"免費憑證"每年可省)

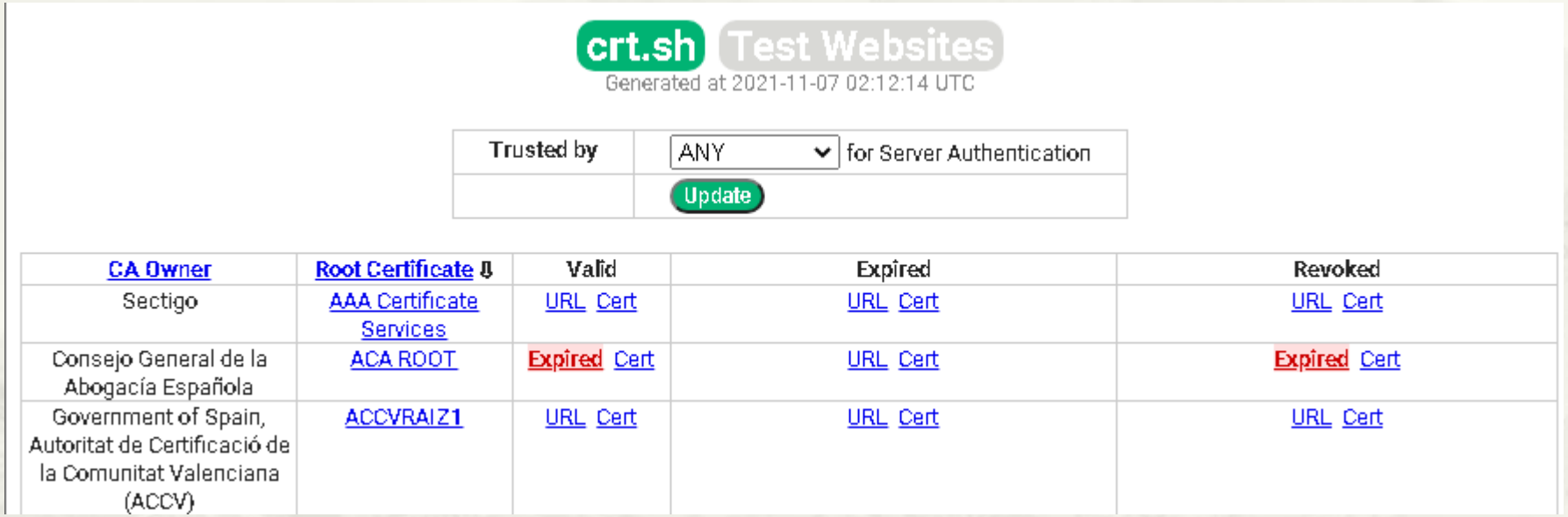
Certificate Populations
https://crt.sh/cert-populations

crt.sh Certificate Populations

CA Owner	Certificates		Precertificates	
	ALL	Unexpired	ALL	Unexpired
Internet Security Research Group	2,176,308,556	246,776,031	1,903,678,250	219,125,328
Sectigo	456,310,973	43,928,339	392,516,336	44,272,084
DigiCert	102,834,932	10,303,709	295,945,021	98,079,405
GoDaddy	16,726,877	836,420	18,587,667	6,716,113
Google Trust Services LLC	13,423,999	1,371,028	78,312,497	4,934,271
GlobalSign nv-sa	6,265,151	162,041	7,694,120	1,502,542
Amazon	4,780,965	1,489,454	30,570,405	20,422,857
Actalis	1,495,501	64,340	2,227,114	732,748
Asseco Data Systems S.A. (previously Unizeto Certum)	1,236,112	44,854	3,344,774	577,809
Start Commercial (StartCom) Ltd.	1,017,817	40	557,448	0
?	827,188	1,439	3,442	699
Entrust	739,568	31,253	1,772,515	553,740
SECOM Trust Systems CO., LTD.	310,956	12,562	247,593	88,122
WoSign CA Limited	258,420	102	75,047	0
QuoVadis	186,047	16,950	2,071,969	1,497,228
SecureTrust	169,385	1,666	44,776	13,182
Microsoft Corporation Core Services Engineering & Operations ("Microsoft CSEO")	156,234	13,406	12,217,668	1,883,204
Buypass	112,210	48,513	108,464	49,430
Deutsche Telekom Security GmbH	91,155	1,579	41,030	21,542
U.S. Federal Public Key Infrastructure (US FPKI)	89,287	1,195	185	18
JPRS	88,606	17,327	179,080	98,338
Government of Spain, Fábrica Nacional de Moneda y Timbre (FNMT)	80,154	794	4,483	2,573
SwissSign AG	70,426	22,620	40,685	22,490
Taiwan-CA Inc. (TWCA)	57,511	3,928	115,251	58,488

Test Websites

* https://crt.sh/test-websites



crt.sh Test Websites

Generated at 2021-11-07 02:12:14 UTC

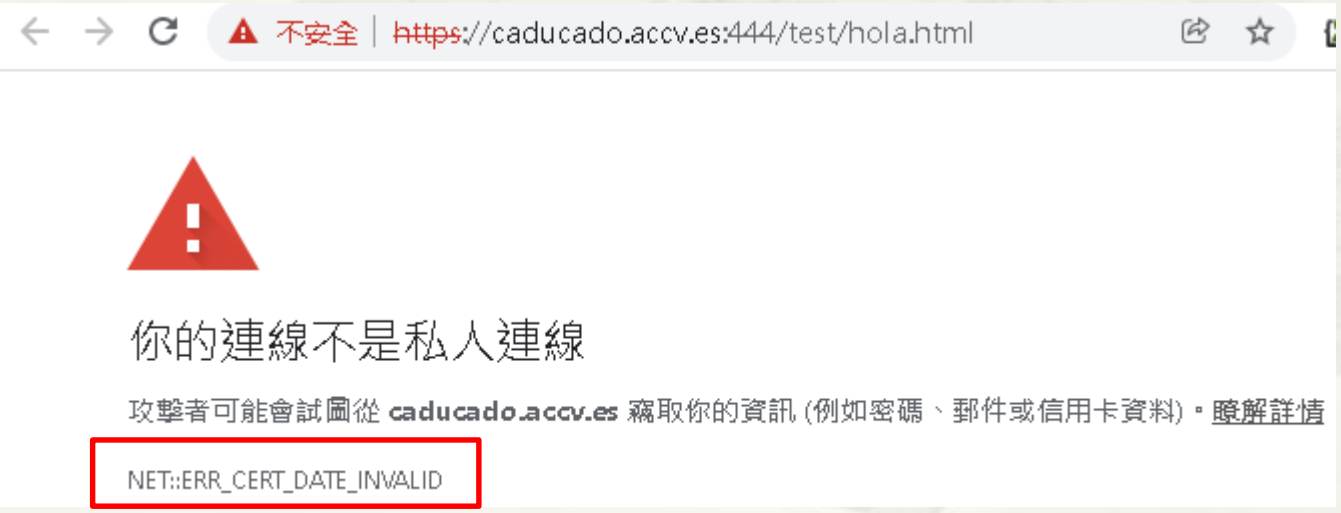
Trusted by: ANY for Server Authentication

Update

CA Owner	Root Certificate	Valid	Expired	Revoked
Sectigo	AAA Certificate Services	URL Cert	URL Cert	URL Cert
Consejo General de la Abogacía Española	ACA ROOT	Expired Cert	URL Cert	Expired Cert
Government of Spain, Autoritat de Certificació de la Comunitat Valenciana (ACCV)	ACCVRAIZ1	URL Cert	URL Cert	URL Cert

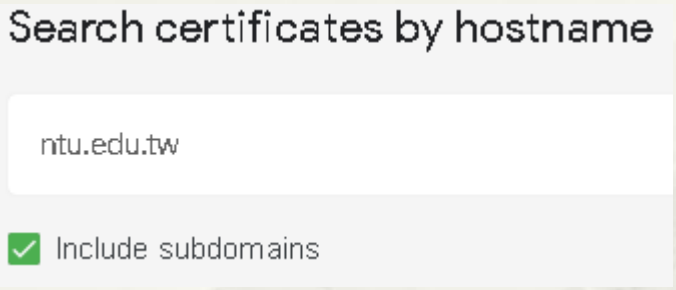
Test Websites

* https://caducado.accv.es:444/test/hola.html
  * NET::ERR_CERT_DATE_INVALID
* https://revocado.accv.es:442/test/hola.html
  * NET::ERR_CERT_REVOKED



Google's Certificate Transparency Lookup Tool

* https://transparencyreport.google.com/https/certificates



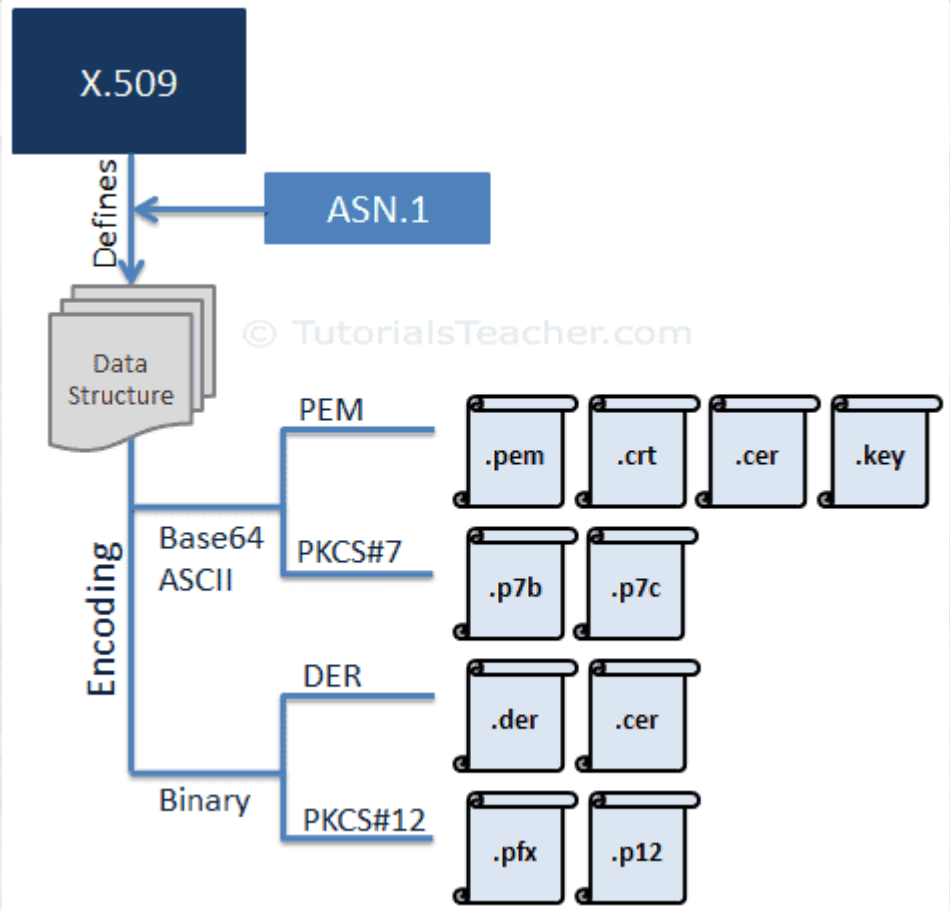
Issuer	# issued
C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	5,843
C=US, O=Let's Encrypt, CN=R3	3,035
C=US, O=cPanel, Inc., L=Houston, ST=TX, CN=cPanel, Inc. Certification Authority	918
C=TW, O=TAIWAN-CA, OU=Secure SSL Sub-CA, CN=TWCA Secure SSL Certification Authority	431
C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA	206
C=GB, O=Sectigo Limited, L=Salford, ST=Greater Manchester, CN=Sectigo RSA Domain Validation Secure Server CA	108
C=TW, O=TAIWAN-CA INC., OU=SSL Certification Service Provider, CN=TWCA Secure CA	71
C=TW, O=TAIWAN-CA INC., OU=SSL Security Services, CN=TWCA Secure Certification Authority	64
C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X1	28
C=GB, O=Sectigo Limited, L=Salford, ST=Greater Manchester, CN=Sectigo RSA Organization Validation Secure Server CA	24
C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority - G2	18
C=TW, O=TAIWAN-CA.COM Inc., OU=SSL Certification Service Provider, CN=TaiCA Secure CA	17
C=US, O=Google Trust Services, CN=GTS CA 1D2	16
C=US, O=Google Trust Services LLC, CN=GTS CA 1D4	15
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High Assurance CA-3	14
C=GB, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, CN=COMODO RSA Domain Validation Secure Server CA	11
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA	9
C=US, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, L=Scottsdale, ST=Arizona, CN=Go Daddy Secure Certificate Authority - G2	9
C=IL, O=StartCom Ltd., OU=StartCom Certification Authority, CN=StartCom Class 1 DV Server CA	6
C=TW, O=TAIWAN-CA, OU=Global EVSSL Sub-CA, CN=TWCA Global EVSSL Certification Authority	5
C=GB, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, CN=UbiquiTLS™ DV RSA Server CA	4
C=ES, O=ips Certification Authority, OU=Certificaciones, L=MADRID, ST=MADRID, CN=ipsCA Level 1 CA	4

Certificate 最長效期

* From September 1st, 2020, several web browsers, led by Apple's Safari will stop trusting SSL certificates issued for longer than 398 days — a 1-year certificate.
  * https://support.apple.com/en-us/HT211025

Certificate Format

Certificate Format



* Ref. https://www.tutorialsteacher.com/https/ssl-certificate-format

Certificate Format

- X509: SSL Certificate Standard
- ASN.1 (Abstract Syntax Notation): Express the Certificate's data structure.
- 編碼格式
  - DER (Distinguished Encoding Rules)
    - Binary Format
    - For Java-based web servers.
    - One Certificate
  - PEM (Privacy Enhanced Mail)
    - Base64 ASCII encoding
    - 以 -----BEGIN ***----- 開頭，以 -----END ***----- 結尾
      - Certificate: ---- BEGIN CERTIFICATE---- and ----END CERTIFICATE----
      - Private key: ---- BEGIN RSA PRIVATE KEY----- and -----END RSA PRIVATE KEY-----
      - Certificate Signing Request: -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----
    - .pem : Include One or Many Certificate and private key
    - .crt .cer .key : One Certificate
    - For Linux Apache

Certificate Format

* PKCS #7(P7B) 密碼編譯訊息語法標準
  * Base64 ASCII encoding
  * Include One or Many Certificate (Without private key.)
  * -----BEGIN PKCS7----- and -----END PKCS7-----
* PKCS #12(PFX) 個人資訊交換
  * Binary Format
  * .pfx : Include One or Many Certificate and private key
  * For Windows IIS

PEM Format Certificate Files

- privkey.pem
  - Private Key for Server Certificate Certificate.
- cert.pem
  - Server Certificate only.
- cert.csr
  - 憑證申請檔 Certificate Signing Request
- chain.pem
  - All certificates that need to be served by the browser excluding server certificate.
  - Intermediate Certificates + Root Certificate(Not Required)
- fullchain.pem
  - All certificates, including server certificate.
  - This is concatenation of chain.pem and cert.pem.
  - Server Certificate + Intermediate Certificates + Root Certificate(Not Required)
- ca_bundle.pem
  - Intermediate Certificates + Root Certificate

Verify Certificate Files

- $ openssl verify ca_bundle.pem
  - ca_bundle.pem: OK
- $ openssl verify cert.pem
  - CN = <your host>
  - error 20 at 0 depth lookup: unable to get local issuer certificate
  - error certificate.pem: verification failed
- $ openssl verify -CAfile ca_bundle.crt certificate.crt
  - certificate.crt: OK

Decode Certificate Files

- Windows 10 Support
  - .cer .crt .der .p7b .pfx
- fullchain.pem 拆解成多張憑證
  - davisyoupc.cc.ntu.edu.tw.crt
  - R3.crt
  - ISRG Root X1_Issuer_DST Root CA X3.crt
  - or
  - ISRG Root X1_Self_Signed.crt

Decode PEM Certificate Files

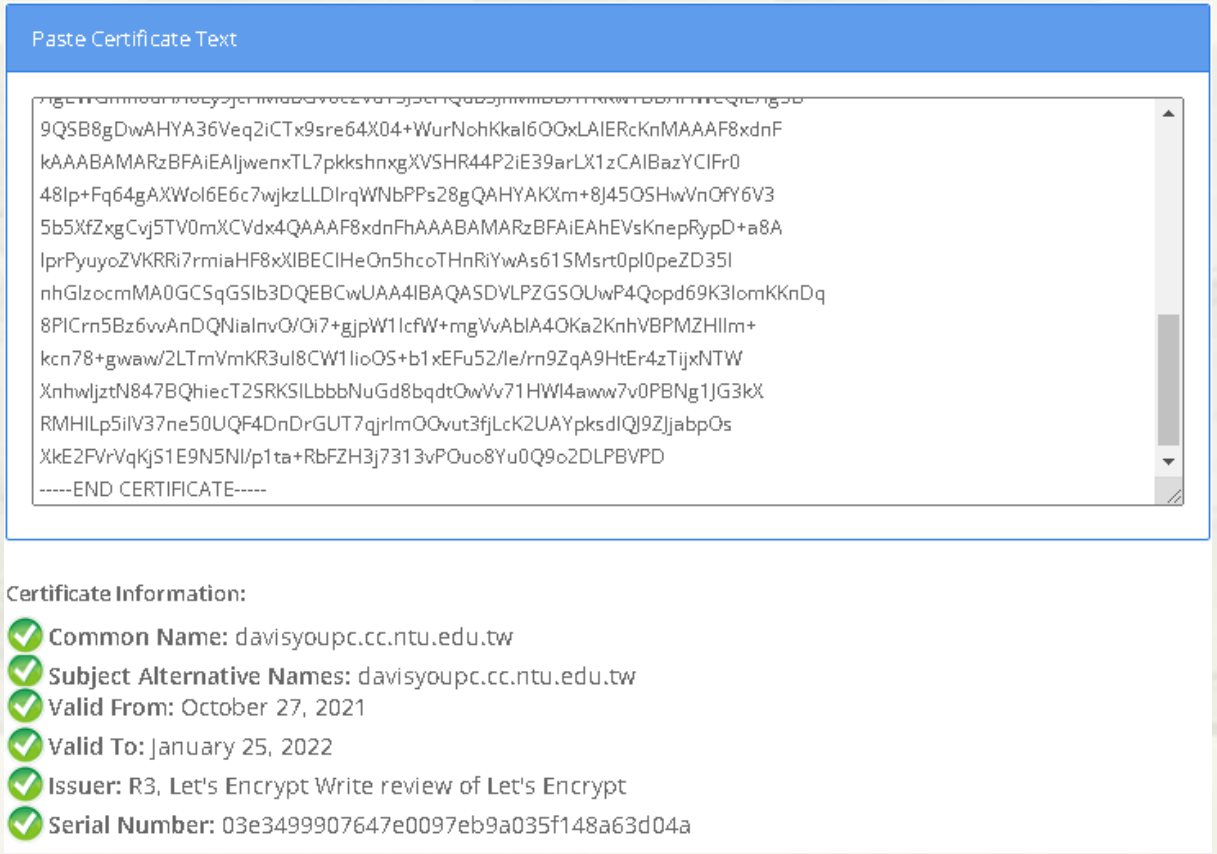
* ~# openssl x509 -in cert.pem -text -noout

  * .pem 若有多個憑證, Only decode first one

* ~# openssl x509 -in cert.pem -noout -issuer
  * issuer=C = US, O = Let's Encrypt, CN = R3
* ~# openssl x509 -in cert.pem -noout -subject
  * subject=CN = *.cc.buda.idv.tw

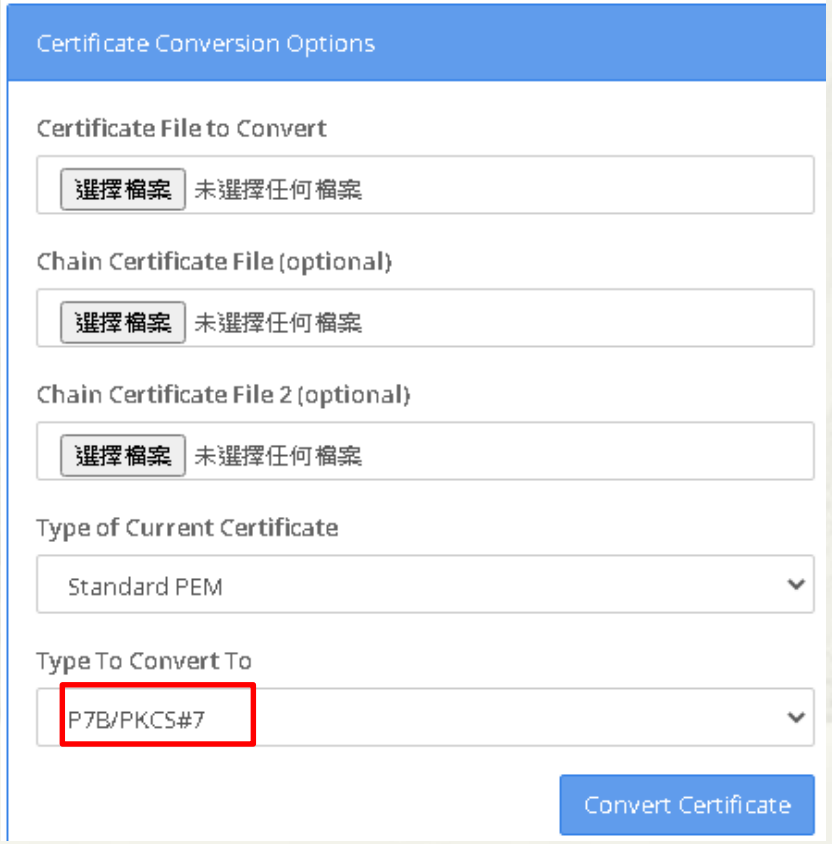
PEM Format Certificate Decoder

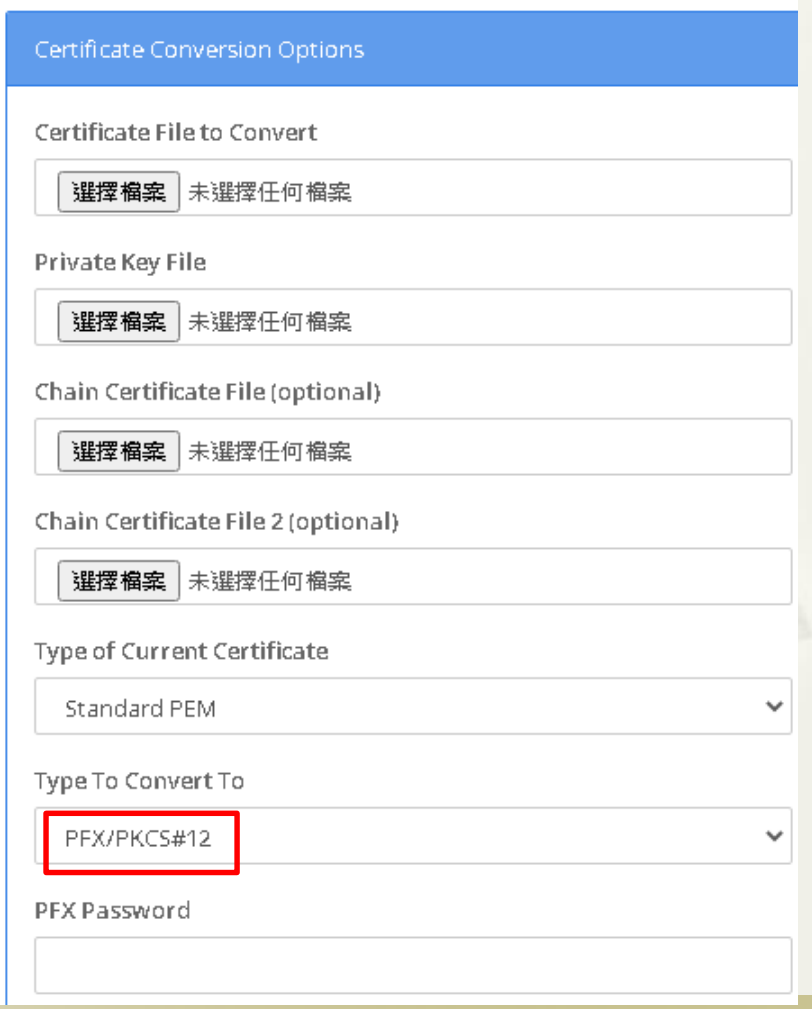
* https://www.sslshopper.com/certificate-decoder.html



Certificate Format Convert

* https://www.sslshopper.com/ssl-converter.html
* From PEM to Others





Certificate Format Convert OpenSSL

- openssl for windows
  - https://wiki.openssl.org/index.php/Binaries
- curl for Windows
  - https://curl.se/windows/
  - OpenSSL 3.0.0 [64bit/32bit]
    - https://curl.se/windows/dl-7.80.0/openssl-3.0.0-win64-mingw.zip
- Ref.
  - https://www.openssl.org/docs/man1.1.1/man1/openssl-pkcs12.html
  - https://www.openssl.org/docs/manmaster/man1/openssl-crl2pkcs7.html

From PEM to Others

- PEM to DER
  - openssl x509 -outform der -in cert.pem -out cert.der
  - 若 .pem 含有多張 Certificates，僅會 Convert First One.
- PEM to PKCS#7
  - openssl crl2pkcs7 -nocrl -out cert.p7b -certfile cert.pem -certfile chain.pem
- PEM to PKCS#12
  - openssl pkcs12 -export -out certificate.pfx -inkey privkey.pem -in cert.pem -certfile chain.pem
    - -inkey filename
      - private key
    - -in filename
      - certificates and private keys in PEM format.
      - The order doesn't matter.
    - -certfile filename
      - additional certificates from

```
Enter Export Password:
Verifying - Enter Export Password:
```

From Others To PEM

- DER to PEM
  - openssl x509 -inform der -in cert.der -out cert.pem
- PKCS #12 to PEM
  - openssl pkcs12 -in keystore.pfx -out keystore.pem -nodes

Root Certificate
根憑證

Root CA & Root Certificate

* Server Certificate 的源頭都是由 Root CA “受信任的根憑證頒發機構” (trusted certificate authority) 所簽發。
* 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，稱為自簽憑證 (Self-signed).
  * 作業系統或瀏覽器出廠時會預載根憑證，存放根憑證的地方稱為 Root Store/Trust Store.

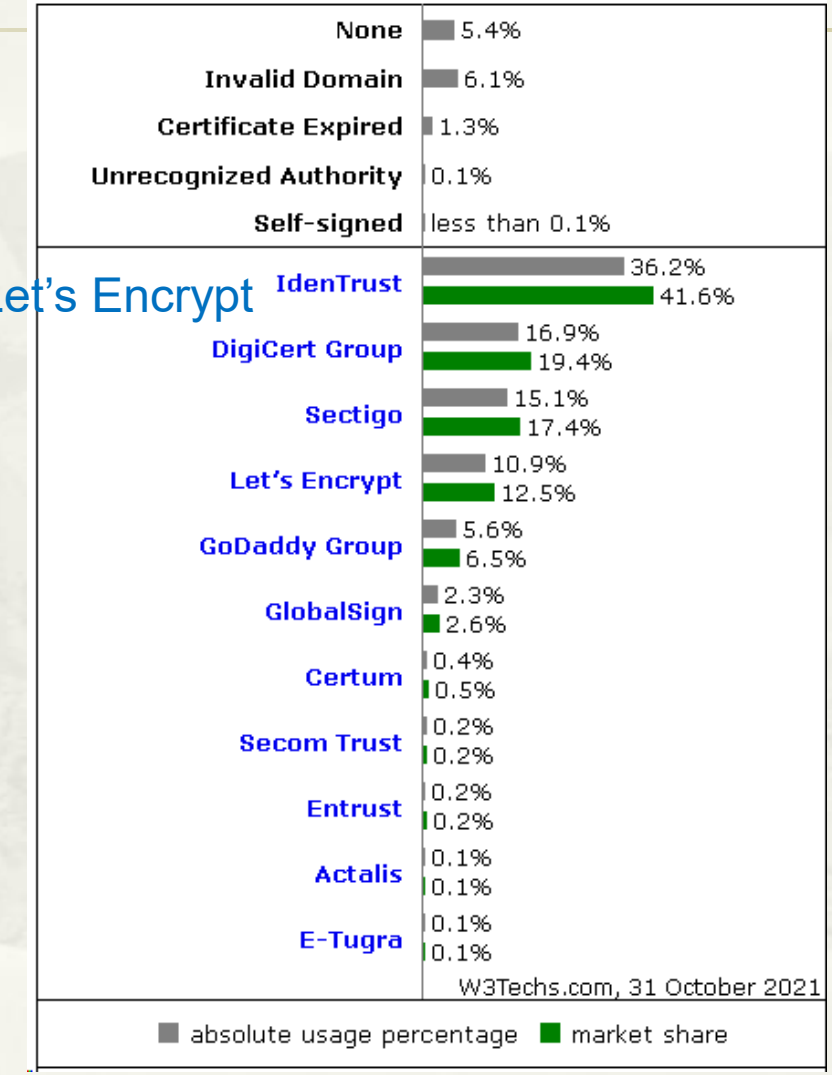
How to Become a Trusted Certificate Authority (Public CA)

- 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
- Invest Immense Resources (Time, Money & People)
- Distribution "Root Certificate" Efforts
  - Get all the browsers, operating systems and applications to trust your certificates
- Ref. https://www.thesslstore.com/blog/how-to-become-a-certificate-authority/

How to Become a Trusted Certificate Authority (Public CA)

* 脆弱的生態系
  * 非階層式授權架構
  * 任一 CA 可發任意 Domain Name 之 Certificate
* MisIssued 原因
  * 歸責於 CA: 駭客攻擊標的
  * 不可歸責於 CA (Man-in-the-middle Attack)
    * DNS Poison
    * BGP poison

Public CAs Market Share June 29, 2021.



Let's Encrypt

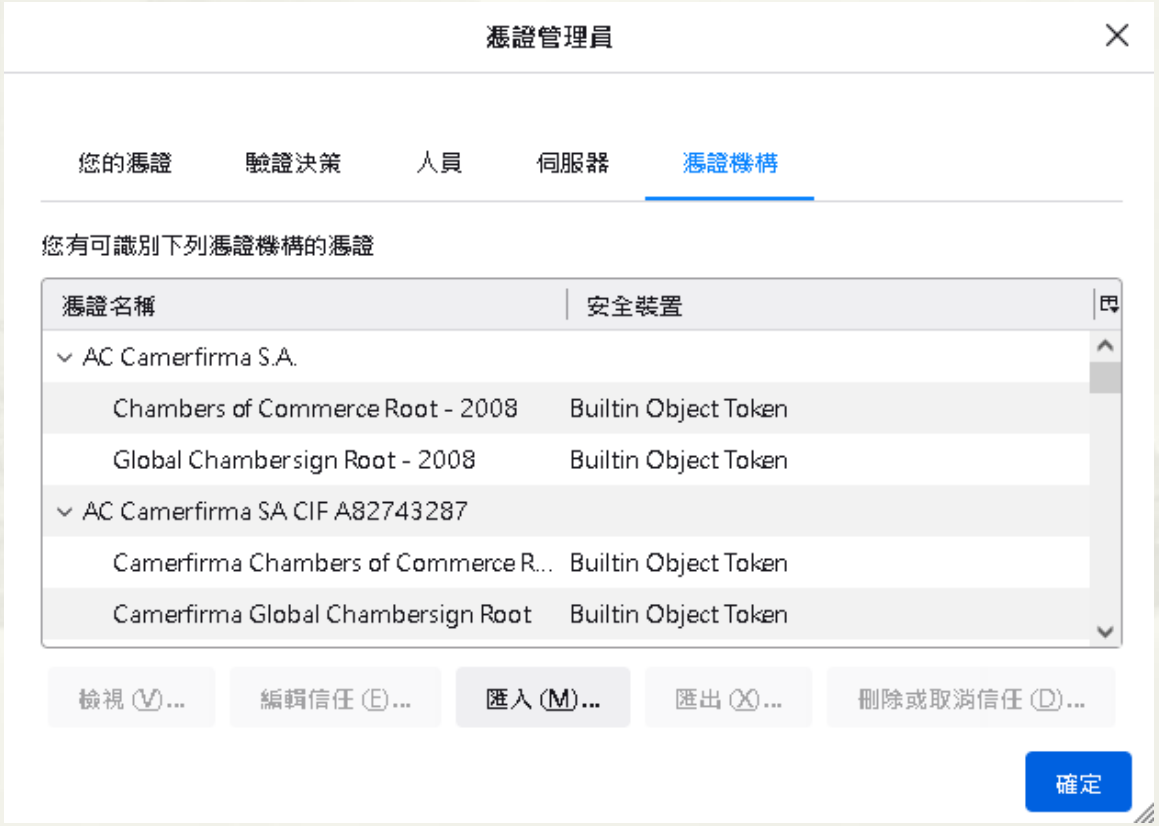
https://w3techs.com/technologies/overview/ssl_certificate

Root Store for Browsers

- Chrome, Safari, Edge, Opera
  - Trust the same root certificates as the operating system.
  - Soon, new versions of Chrome will also have their own root store.
    - https://www.chromium.org/Home/chromium-security/root-ca-policy
- Firefox
  - It has its own root store.

Root Store for Firefox

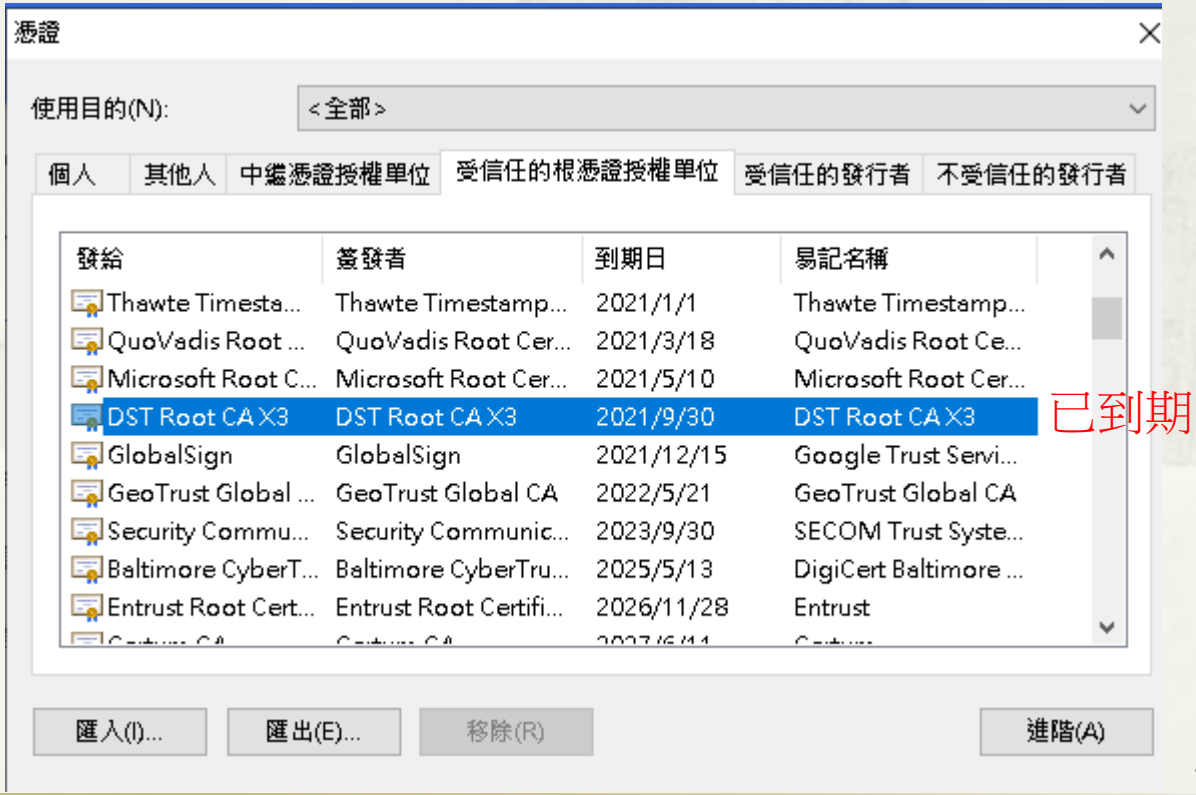
- Firefox Included CA List
  - https://wiki.mozilla.org/CA/Included_CAs
- about:preferences#privacy > 檢視憑證(Button)



- about:preferences#advanced > View Certificate (舊版)

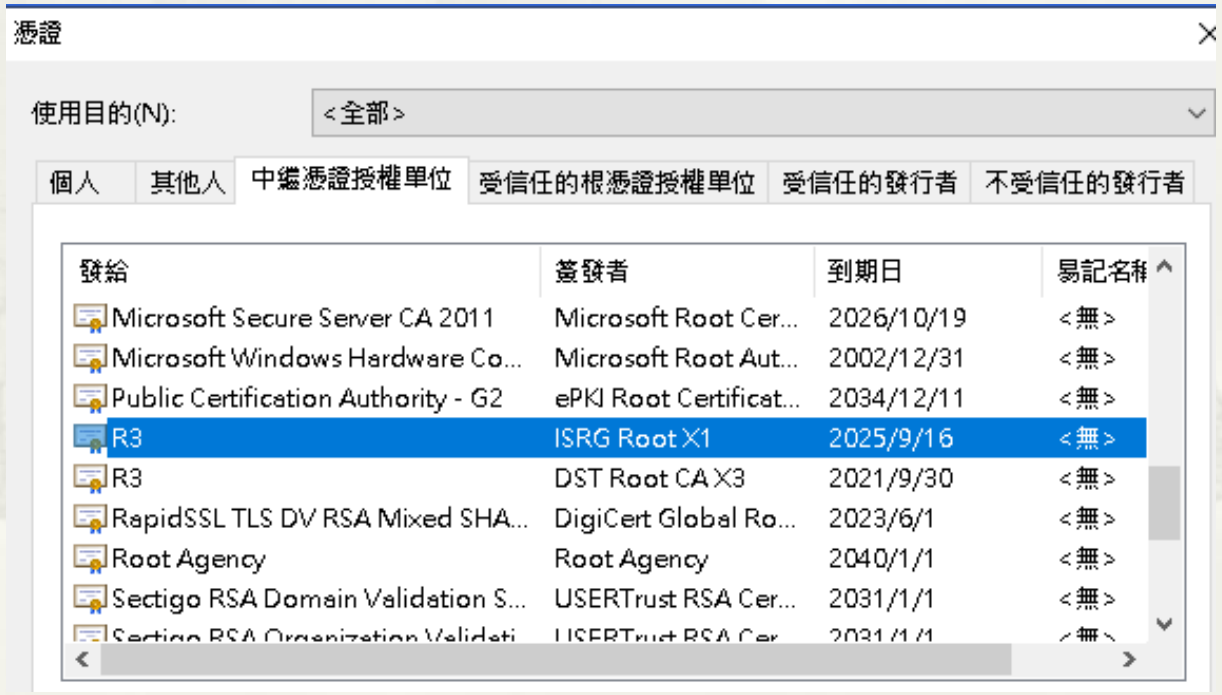
Root Store for Chrome

* chrome://settings/security > 管理憑證
* 根憑證



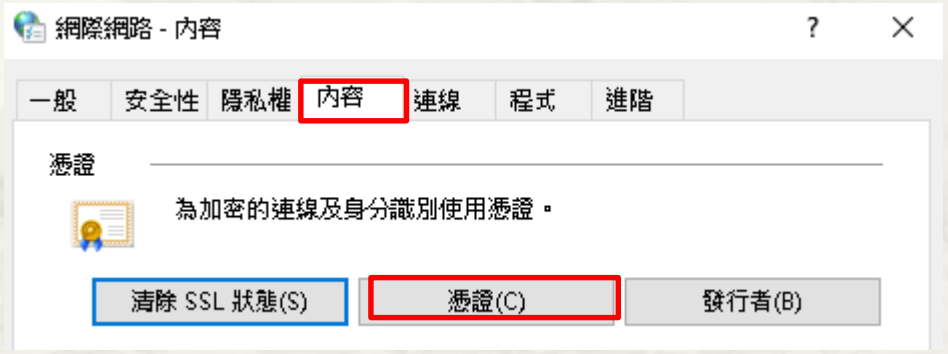
已到期

* 中繼憑證



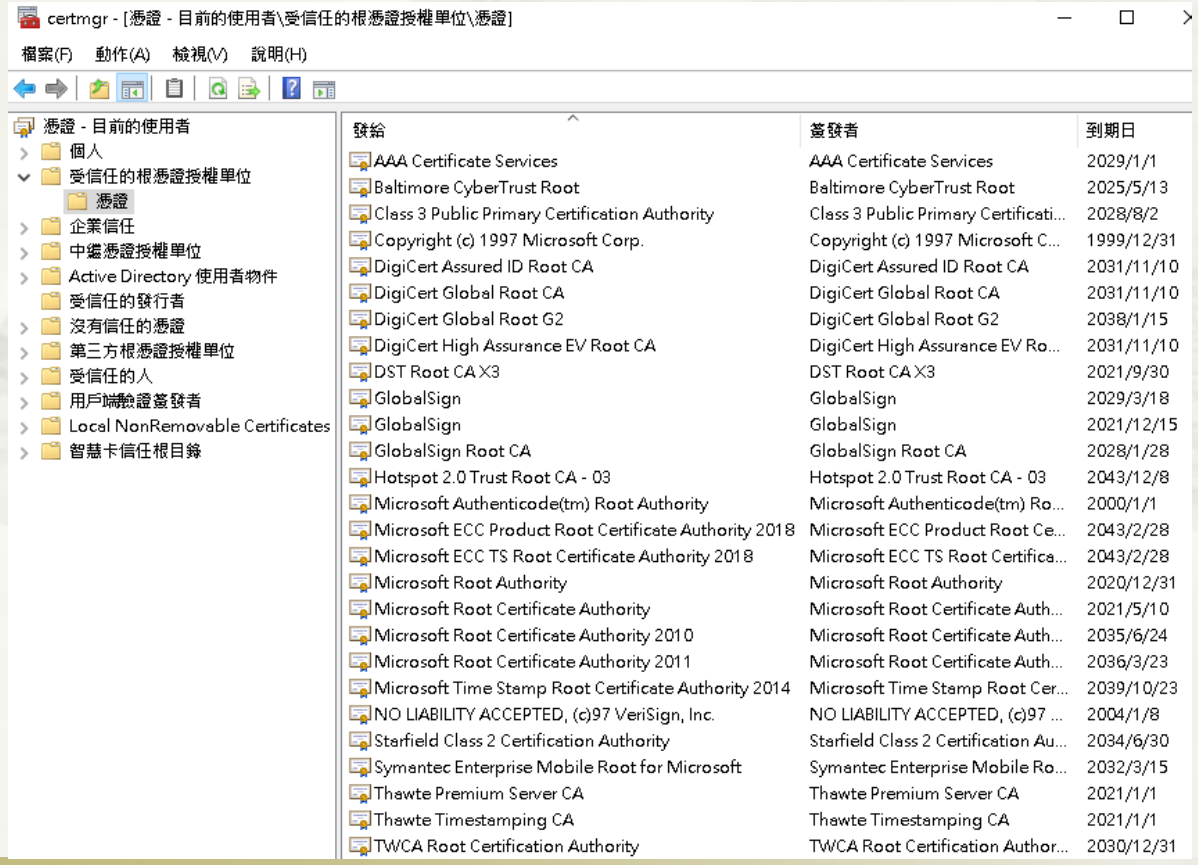
Root Store for Windows10
方法1

* 控制台 > 網路和網際網路 > 網際網路選項
* or
* inetcpl.cpl

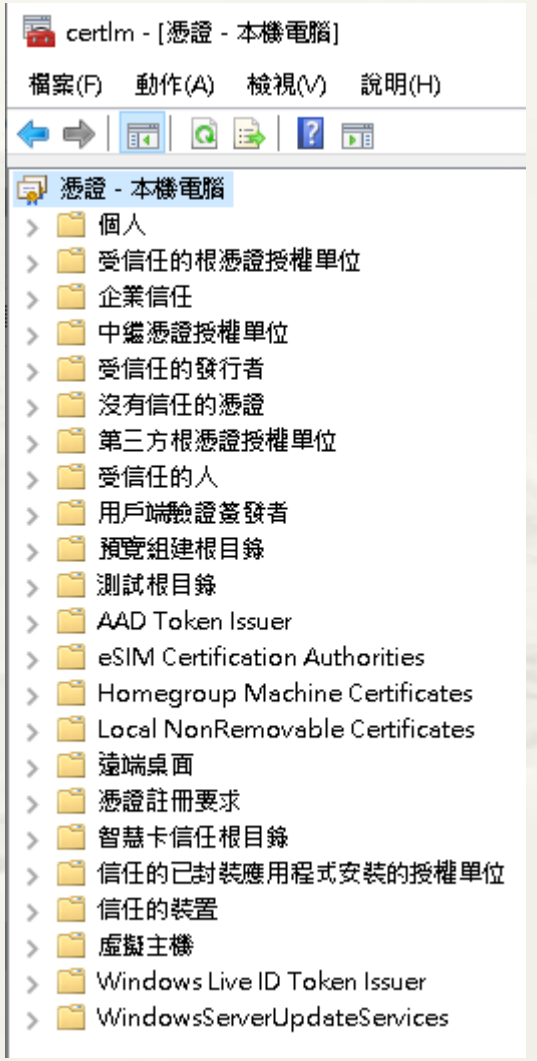


Root Store for Windows10
方法2

* certmgr.msc
  * 使用者帳戶

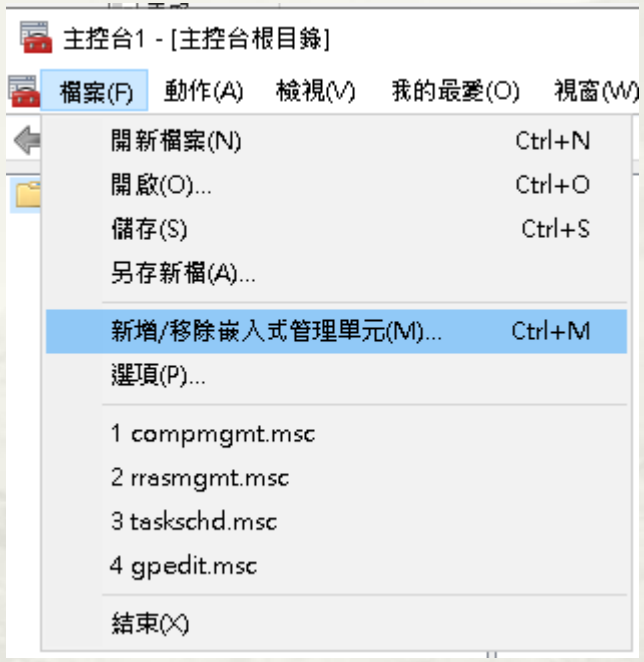


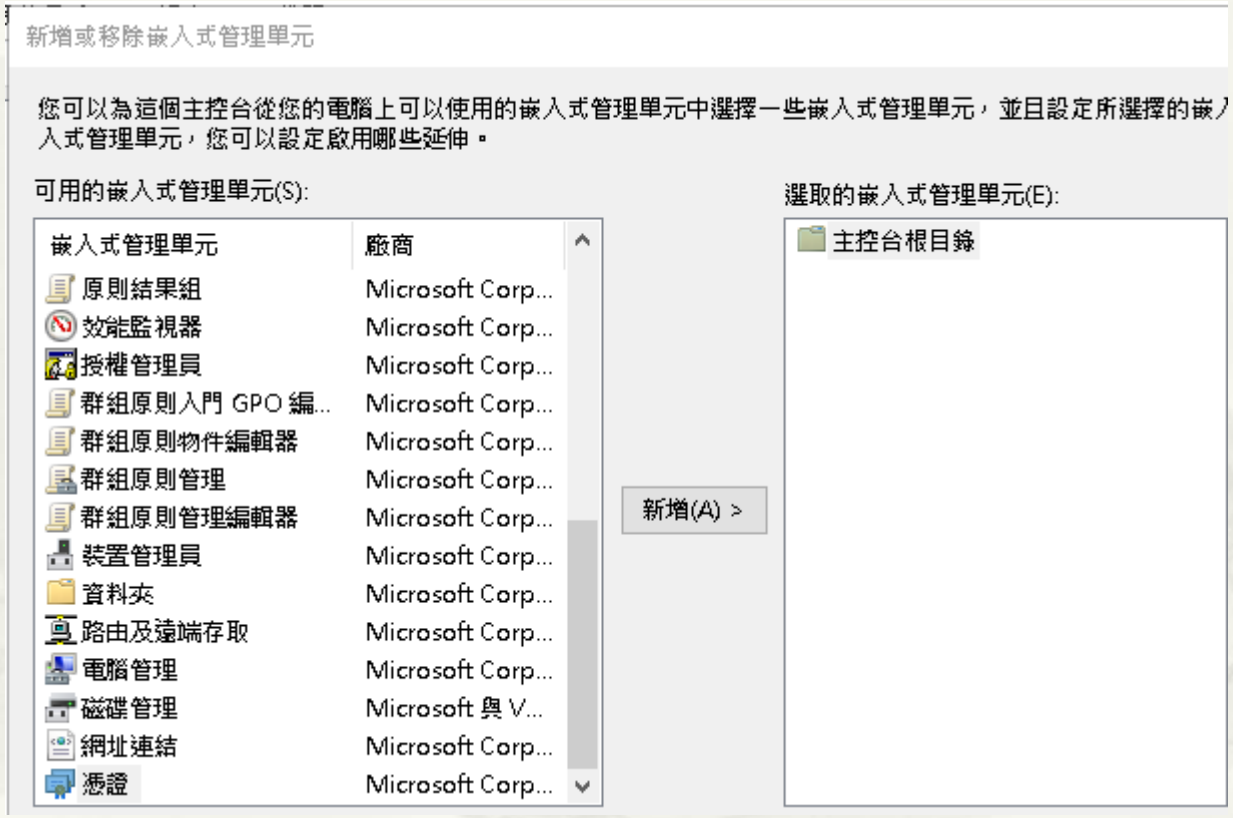
* certlm.msc
  * 電腦帳戶



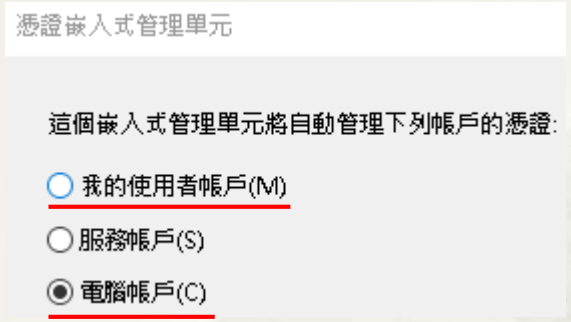
Root Store for Windows10
方法3

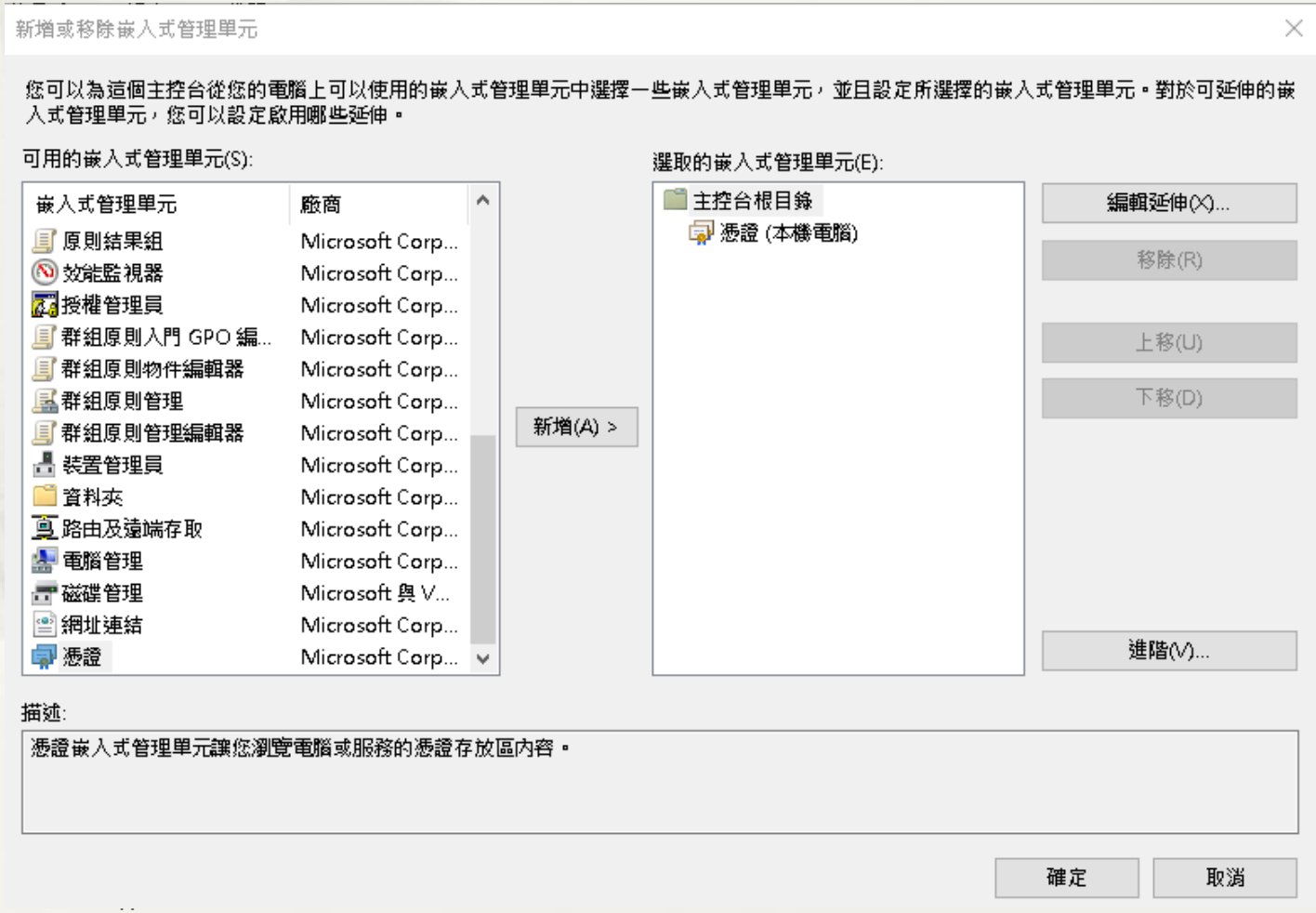
* 開始 -> 執行: mmc





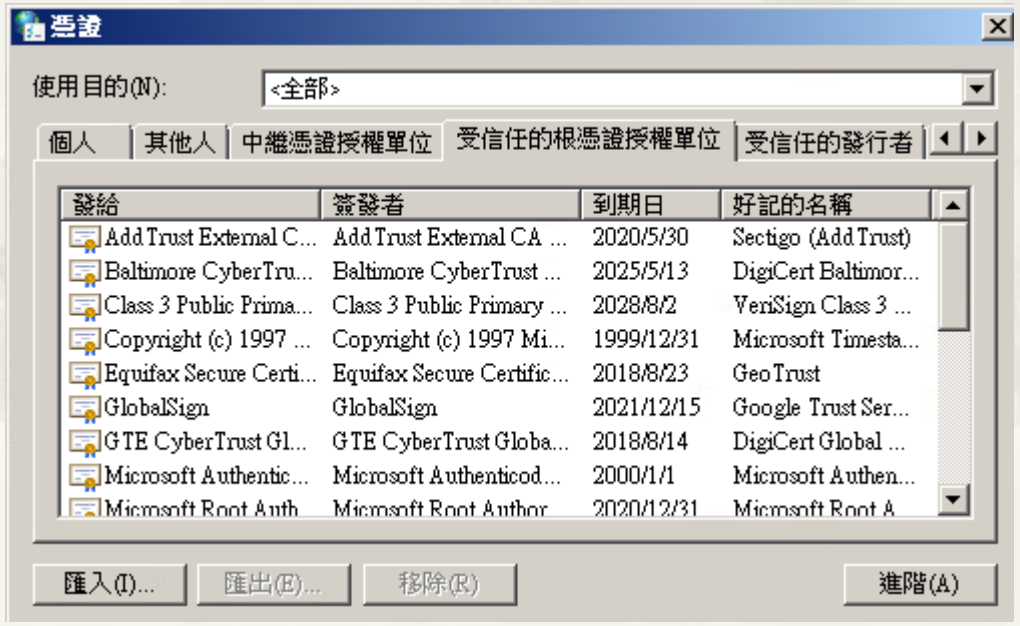
Root Store for Windows10
方法3





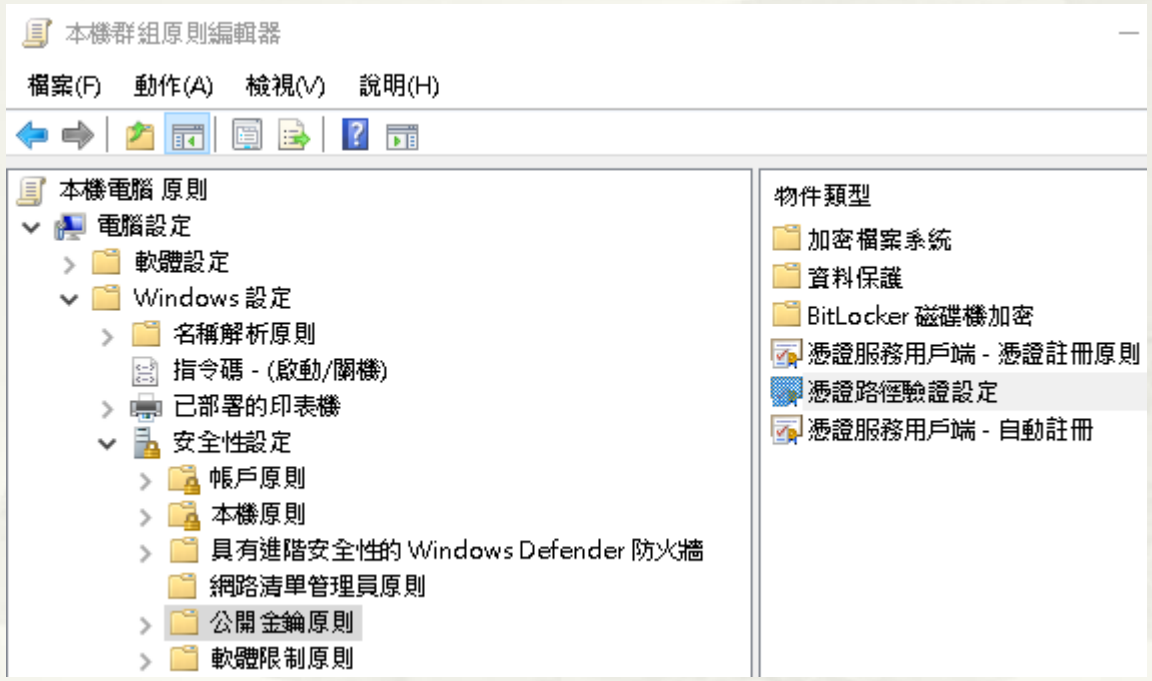
Root Store Update

* 經測試 Win7 SP1 原始版
  * 使用 IE, Chome 瀏覽網頁後, 會將缺少的根憑證自動安裝於 Root Store



Root Store Update

* 更新規則



Root Store for curl

- curl -v https://www.ntu.edu.tw
- Curl for Windows
  - https://curl.se/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
```

- Curl built-in for Ubuntu

```
* 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
```

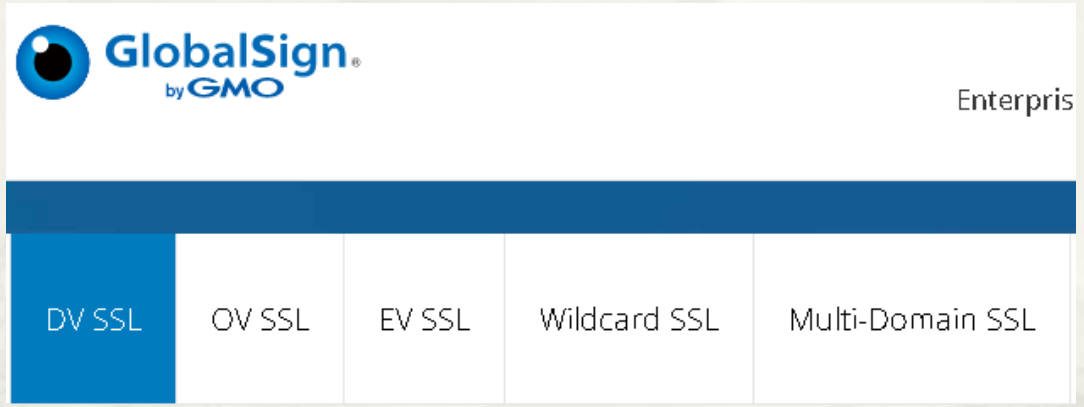
Certificate Type

Certificate Type

* https://www.pumo.com.tw/www/security/spec/spec.html

	TWCA SSL 伺服器數位憑證	TWCA SAN SSL 伺服器數位憑證	TWCA EV SSL 伺服器數位憑證
最高256-bit 加密強度	✓	✓	✓
完整組織 身分驗證	✓	✓	✓
2048-bit 根憑證	✓	✓	✓
99%+ 瀏覽器支援	✓	✓	✓
3A認證 自主管理服務			
EV驗證 綠色網址列			✓
支援SAN 多網站名稱		✓	

* https://shop.globalsign.com/en/ssl/domain-ssl



Certificate Type and Price

* TWCA

憑證類別	價格 NT
單一網域 SSL 憑證	7000
SAN SSL 憑證 (3個獨立主網域)	25,000
Wildcard SSL憑證	55,000
EV SSL 憑證	30,000

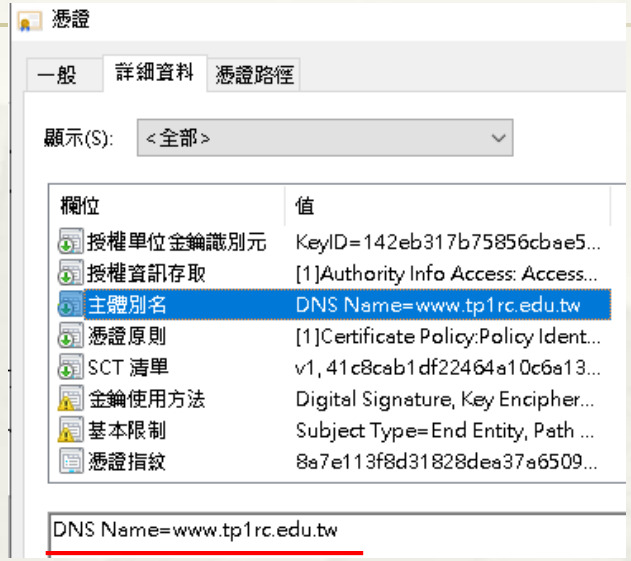
* https://www.pumo.com.tw/www/security/ssl-solution.jsp

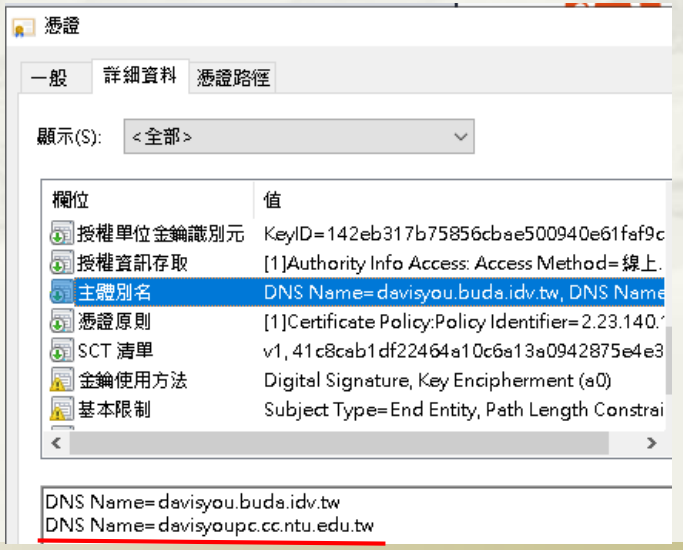
Certificate Type

* Domain Name
  * One Domain
  * Multiple Domains
  * Wildcard Domain
* Trust Level
  * Domain Validated(DV)
  * Organization Validation (OV)
  * Extended Validation (EV)

One/Multiple/Wildcard Domain

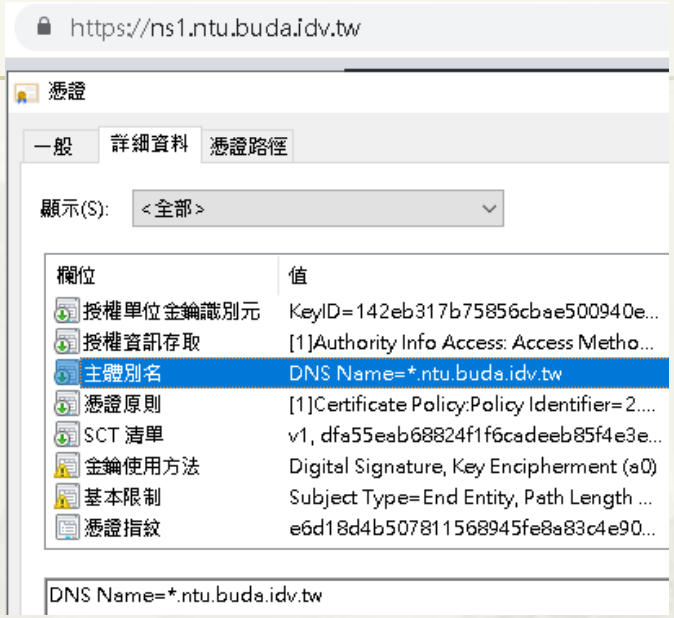
- One Domain
  - https://crt.sh/?id=5372942977
  - X509v3 Subject Alternative Name:
    - DNS:www.tp1rc.edu.tw
- Multiple Domain(SAN)
  - Up to 100 different domain names
  - https://crt.sh/?id=
    - X509v3 Subject Alternative Name:
    - DNS:ns1.ntu.buda.idv.tw
    - DNS:ns2.ntu.buda.idv.tw
  - https://crt.sh/?id=5572136554
    - X509v3 Subject Alternative Name:
    - DNS:davisyou.buda.idv.tw
    - DNS:davisyoupc.cc.ntu.edu.tw

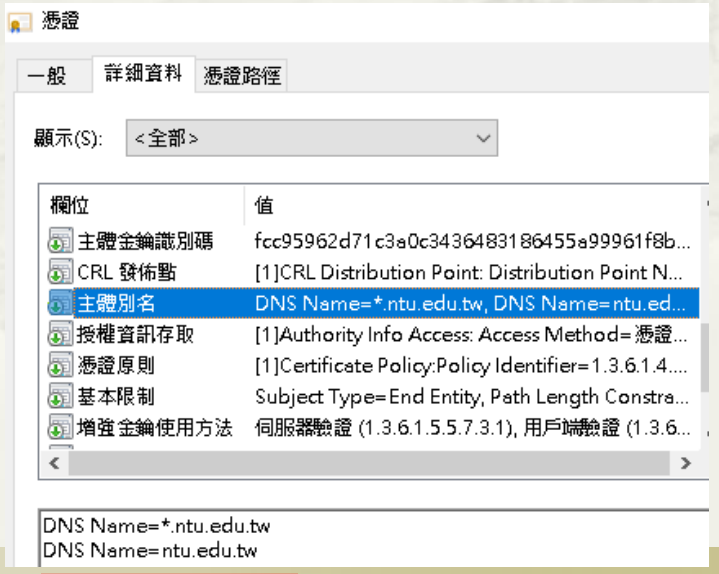




One/Multiple/Wildcard Domain

- Wildcard Domain
  - Let’s Encrypt
    - https://crt.sh/?dNSName=*.ntu.buda.idv.tw
      - X509v3 Subject Alternative Name:
        - DNS:*.ntu.buda.idv.tw
    - https://crt.sh/?dNSName=*.davis.cc.ntu.edu.tw
      - X509v3 Subject Alternative Name:
        - DNS:*.davis.cc.ntu.edu.tw
  - TWCA
    - https://crt.sh/?dNSName=*.ntu.edu.tw
      - X509v3 Subject Alternative Name:
        - DNS:*.ntu.edu.tw
        - DNS:ntu.edu.tw



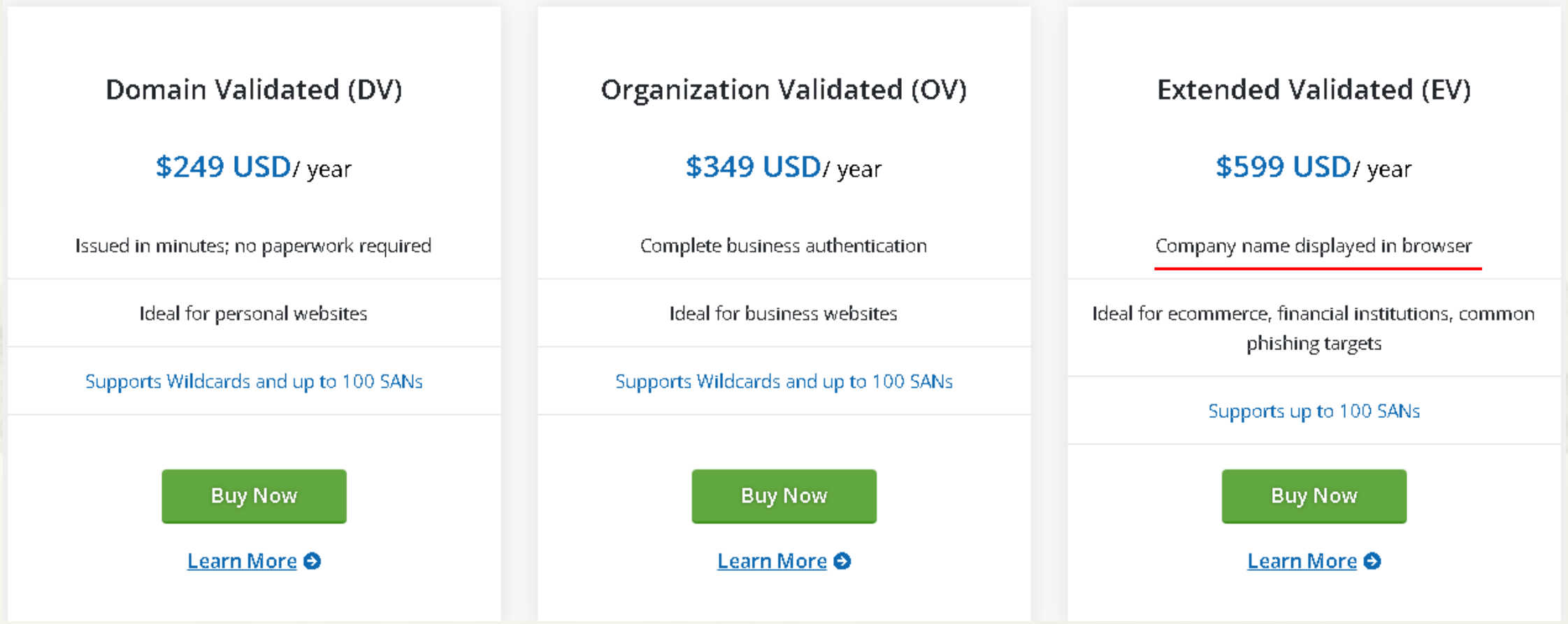


Certificate Trust Level

- Domain Validated(DV)
  - CA will only verify the domain name, and not verify anything additional.
  - Issued immediately
- Organization Validation (OV)
  - CA will make sure that the applicant actually has the right to the specific domain name plus the CA does some vetting (investigation) of the said organization.
  - Takes about 2 days to issue.
- Extended Validation (EV)
  - CA will make sure that the applicant actually has the right to the specific domain name plus the CA conducts a very thorough vetting (investigation) of the organization.
  - legal, physical & operational existence of the entity and identity of the entity matches official records
  - Takes about 10 days to issue.

Certificate Trust Level

* https://shop.globalsign.com/en/ssl-tls-certificates



Certificate Trust Level

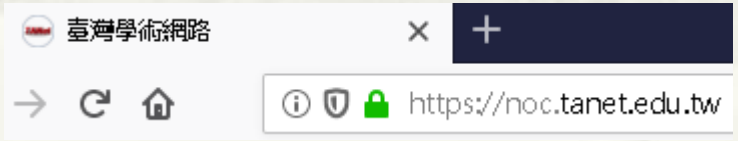
* https://www.pumo.com.tw/www/security/ssl-comparison.jsp

	SSL EV 憑證	SSL OV 憑證	SSL DV 憑證
	EV (Extended validation) 擴展層級驗證	OV (Organization validated) 組織層級驗證	DV (Domain validated) 網域層級驗證
憑證介紹	為最高等級認證，需通過網域、組織 (電話)、通過五大會計事務所之一驗證，審核方式嚴謹。各瀏覽器網址列安全顯示公司名稱 如：TWCA，屬 EV 等級。	公司組織等級認證，除網域認證外，還有公司資訊驗證 (電話驗證)。 如：中華電信，屬 OV 等級。	最低等級的 SSL 憑證，僅有網域所有權認證。 如： GeoTrust、RapidSSL 兩者也屬DV 等級 Let's encrypt 為免費憑證 (雖為免費憑證但後續無賠償金額的機制)
價格	高	中等	低
安全性	高	中等	低
消費者保障	高 (消費者能知道營運網站的企業名稱，且能確認是否為合法立案的真實企業)	中等 (消費者僅能知道營運網站的企業名稱，但無法確認是否為真實企業)	無 (消費者無法辨識網站是否為真實企業經營)

What's the Difference?

* Before Firefox 69
  * https://ftp.mozilla.org/pub/firefox/releases/69.0/win64/en-US/
  * https://www.tp1rc.edu.tw/

  * https://noc.tanet.edu.tw/



* https://crt.sh/

* https://www.digicert.com

* https://www.globalsign.com/

Browsers Remove Extended Validation Indicators

* 13 AUGUST 2019
  * After Chrome 77
  * After Firefox 70
* https://duo.com/decipher/chrome-and-firefox-removing-ev-certificate-indicators
* https://sectigo.com/resource-library/root-causes-144-whatever-happened-to-the-green-address-bar

如何辨識 Certificate Trust Level

- Certificate Object Identifier (OID)
  - Each CA uses a different OID to assert extended validation.
  - Each user agent must have a list of OIDs that indicate extended validation.
- Search OID
  - https://oidref.com
  - https://oid-info.com
- Search word in OID listings
  - https://www.alvestrand.no/objectid/top.html
    - https://www.alvestrand.no/cgi-bin/hta/oidwordsearch?text=Taiwan

Domain/Organization/Extended Validation

* https://oidref.com/2.23.140.1

Reference record for OID 2.23.140.1

2 joint-iso-itu-t, joint-iso-ccitt > 23 international-organizations > 140 ca-browser-forum > 1 certificate-policies

Children (3)

OID	Name	Sub children	Sub Nodes Total	Description
2.23.140.1.1	ev-guidelines	0 EV	0	Extended Validation (EV) guidelines certificate policy
2.23.140.1.2	baseline-requirements	2	2	Digital certificate's and issuing Certificate Authority's compliance with the CA/Browser Forum's baseline requirements
2.23.140.1.4	code-signing-requirements	1	1	Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

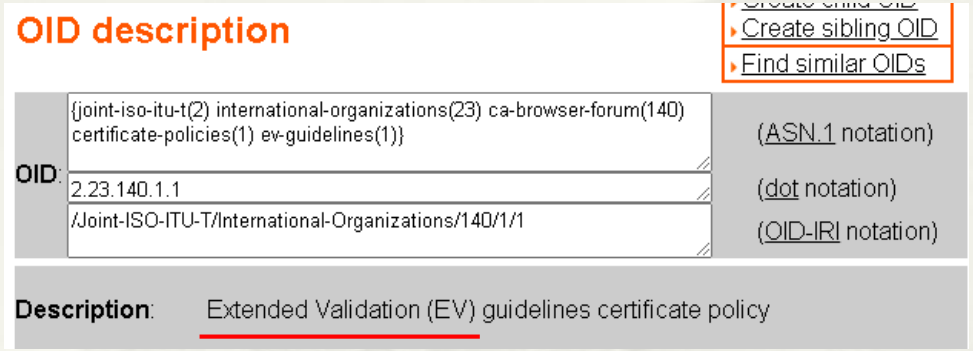
* https://oidref.com/2.23.140.1.2

Children (2)

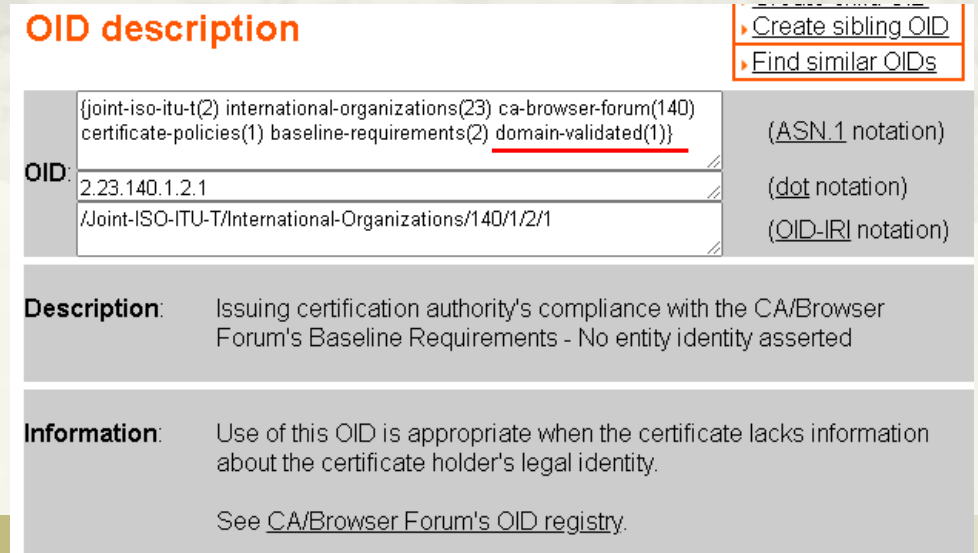
OID	Name	Sub children	Sub Nodes Total	Description
2.23.140.1.2.1	domain-validated	0 DV	0	Issuing certification authority's compliance with the baseline requirements
2.23.140.1.2.2	subject-identity-validated	0 OV	0	Corresponding certificate issued in accordance with the CA/Browser Forum's baseline requirements

Domain/Organization/Extended Validation

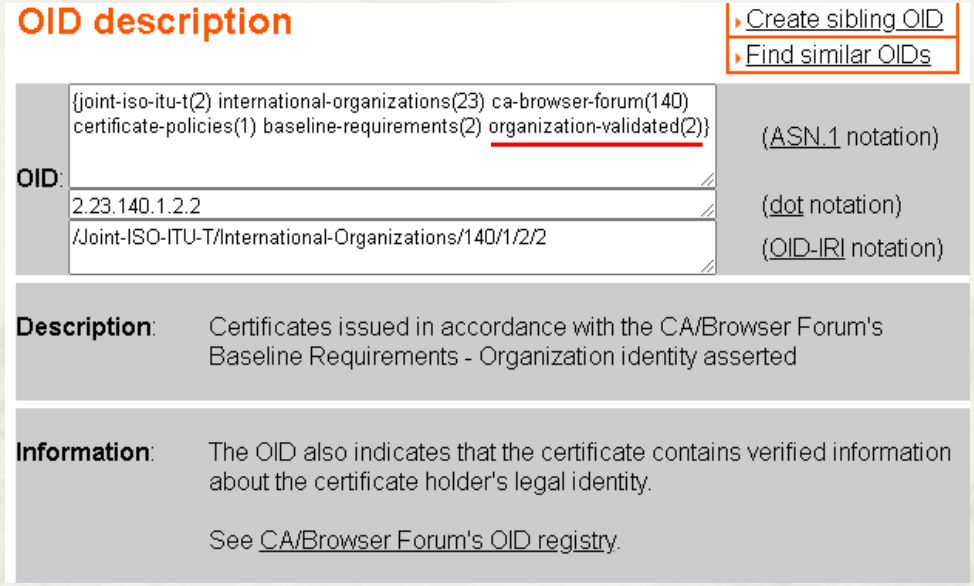
* EV http://oid-info.com/get/2.23.140.1.1



* DV http://oid-info.com/get/2.23.140.1.2.1



* OV http://oid-info.com/get/2.23.140.1.2.2

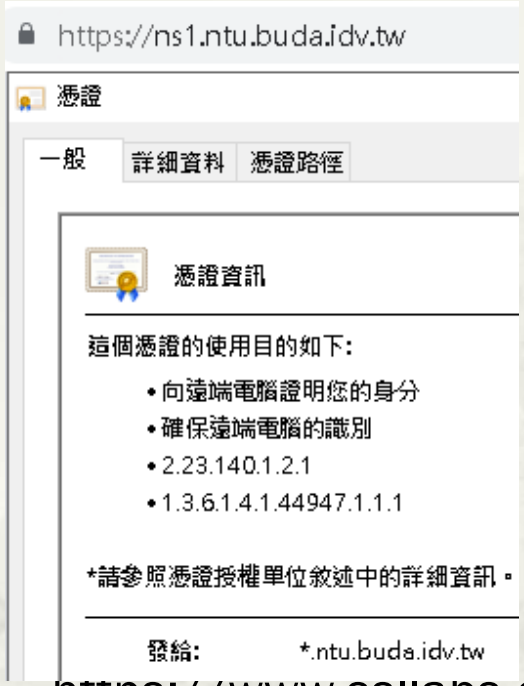


X509v3 Certificate Policies

* Certificate for https://www.tp1rc.edu.tw
  * https://crt.sh/?id=5372942977

```
X509v3 Subject Alternative Name:
    DNS:www.tp1rc.edu.tw
X509v3 Certificate Policies:
    Policy: 2.23.140.1.2.1
    Policy: 1.3.6.1.4.1.44947.1.1.1
      CPS: http://cps.letsencrypt.org
```

Certificate OID
Let's Encrypt (DV)



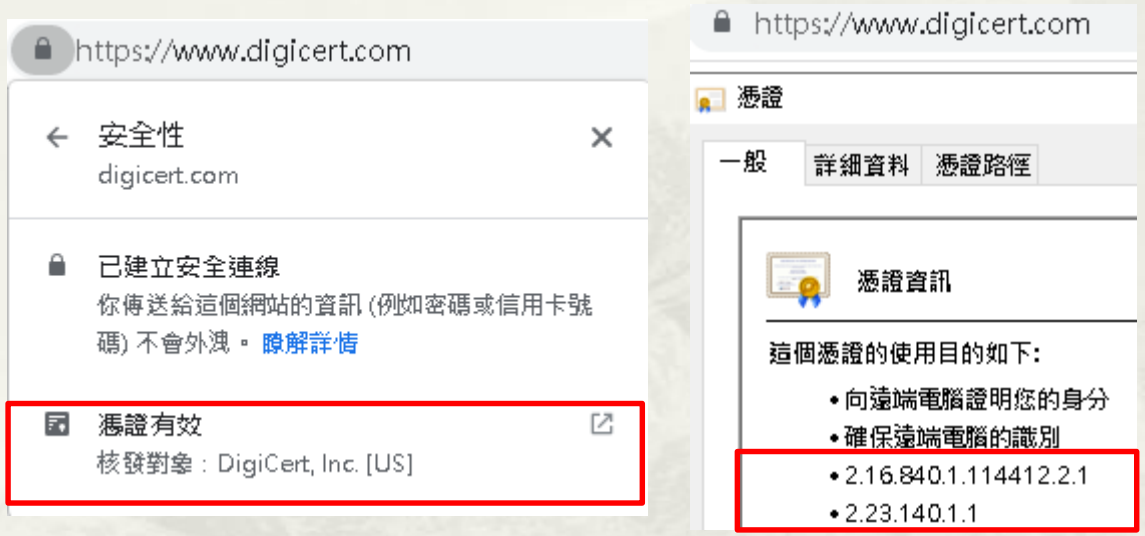
- https://www.ssllabs.com/ssltest/analyze.html?d=www.tp1rc.edu.tw&s=140.112.2.208&latest

Extended Validation	No

- https://oidref.com/1.3.6.1.4.1.44947
  - {iso(1) iso-identified-organization(3) dod(6) internet(1) private(4) enterprises(1) 44947(44947)}
- http://oid-info.com/get/1.3.6.1.4.1.44947
  - Description: Internet Security Research Group
  - Information: This OID is used by Let's Encrypt.

Certificate OID
DigiCert (EV)

* https://www.digicert.com/



* https://www.ssllabs.com/ssltest/analyze.html?d=www.digicert.com&latest

Extended Validation	Yes

* https://crt.sh/?id=4836494933
  * X509v3 Certificate Policies:
    * Policy: 2.16.840.1.114412.2.1
    * Policy: 2.23.140.1.1
* http://oid-info.com/get/2.16.840.1.114412.2.1
  * Description:DigiCert Extended Validation (EV) SSL/TLS certificates
* https://oidref.com/2.16.840.1.114412.2.1
  * {joint-iso-itu-t(2) country(16) us(840) organization(1) digicert(114412) ev-ssl-certificates(2) 1(1)}

Certificate OID
GlobalSign (EV)

* https://www.globalsign.com/en

* https://www.ssllabs.com/ssltest/analyze.html?d=www.globalsign.com

Extended Validation	Yes

* https://oidref.com/1.3.6.1.4.1.4146.1.1
  * {iso(1) iso-identified-organization(3) dod(6) internet(1) private(4) enterprises(1) 4146(4146) certificate-policies(1) extended-Validation-SSL(1)}

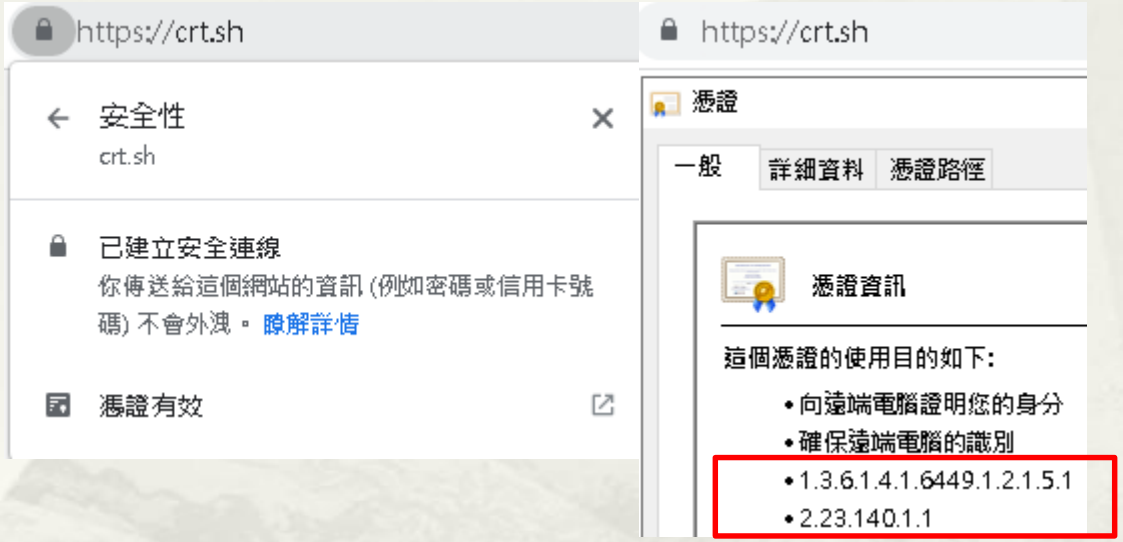
http://oid-info.com/get/1.3.6.1.4.1.4146.1.1

Current Registration Authority

Name:	PACOM1 CA Governance
Address:	GlobalSign NV/SA Diestsevest 14 3000 Leuven Belgium

Certificate OID
Sectigo Limited (EV)

* https://crt.sh/



* https://www.ssllabs.com/ssltest/analyze.html?d=crt.sh

Extended Validation	Yes

* http://oid-info.com/get/1.3.6.1.4.1.6449.1.2
  * Description: Sectigo Limited
* https://oidref.com/1.3.6.1.4.1.6449.1.2
  * {iso(1) iso-identified-organization(3) dod(6) internet(1) private(4) enterprises(1) 6449(6449) certificates(1) policies(2)}

Let's Encrypt

* Will Certbot issue Extended Validation (EV) certificates?
  * Certbot and Let's Encrypt have no plans to issue EV certificates at this time.

OID 補充

* https://oid.nat.gov.tw/OIDWeb/

大學搜尋結果共28筆

首頁 > 物件識別碼（OID）查詢

查詢結果：

- 中央警察大學
- 國防大學
- 國防大學國防管理學院
- 國防大學理工學院
- 國立中山大學附屬國光高級中學
- 國立中央大學附屬中壢高級中學
- 國立中興大學附屬高級中學
- 國立中興大學附屬臺中高級農業職業學校
- 國立屏東大學附設實驗國民小學
- 國立政治大學附屬高級中學
- 國立高雄師範大學附屬高級中學
- 國立清華大學附設實驗國民小學
- 國立嘉義大學附設實驗國民小學
- 國立彰化師範大學附屬高級工業職業學校
- 國立暨南國際大學附屬高級中學
- 國立臺中教育大學附設實驗國民小學
- 國立臺北科技大學附屬桃園農工高級中等學校
- 國立臺北教育大學附設實驗國民小學
- 國立臺東大學附屬特殊教育學校
- 國立臺東大學附屬體育高級中學
- 國立臺南大學附設實驗國民小學
- 國立臺南大學附屬高級中學
- 國立臺南大學附屬啟聰學校
- 國立臺灣師範大學附屬高級中學
- 國立東華大學附設實驗國民小學
- 國立高雄餐旅大學附屬餐旅高級中等學校
- 國立臺東大學附設實驗國民小學

中央警察大學	
機關代號	301210000T
機關OID	2.16.886.101.20003.20001.20009

* https://oidref.com/2.16.886

Children (3)

OID	Name	Sub children	Sub Nodes Total	Description
2.16.886.1	illegal	2	6	Supposed to be assigned to Chunghaw Telecom co. but the parent node is **illegally** used by Taiwan
2.16.886.2	illegal	0	0	Supposed to be assigned to Computer & Communications Research Lab. of Industrial Technology Research Institute but the pare…
2.16.886.101	illegal-gov	1	7	Government Root Certification Authority of Taiwan This OID is **illegal** because country code 886 is illegally used by Taiwan.

Brothers (201)

To many brothers! Only 100 nearest brothers are shown.

OID	Name	Sub children	Sub Nodes Total	Description
…				
2.16.840	us	1	16441	United States of America
2.16.854	bf	0	0	Burkina Faso
2.16.858	uy	3	6	Uruguay
2.16.860	uz	0	0	UZBEKISTAN
2.16.862	ve	1	2	Venezuela
2.16.882	ws	0	0	SAMOA
2.16.887	ye	0	0	Yemen
2.16.891	891	0	0	Serbia and Montenegro (code not in current use)
2.16.894	zm	0	0	Zambia
…				

簡報完畢
謝謝