

# Certificate Chain

---

臺灣大學計資中心

網路組

游子興

The background features a large, semi-circular fan with a traditional Chinese landscape painting. The painting depicts a mountainous region with a river, trees, and buildings. The fan is positioned centrally on the page, and the text is overlaid on it.

# **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](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

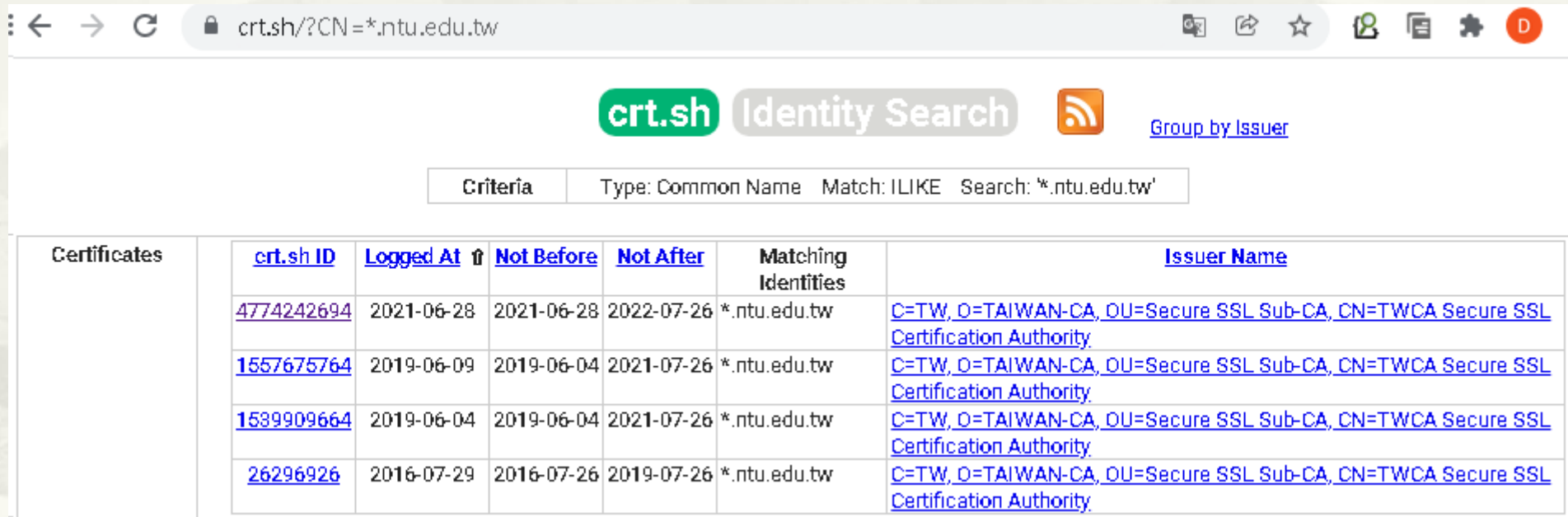
\* <https://crt.sh/?CN=www.tp1rc.edu.tw>

The screenshot shows the crt.sh website interface. At the top, there is a search bar with the text 'Identity Search' and a search button. Below the search bar, there is a search criteria box showing 'Criteria Type: Common Name Match: ILIKE Search: 'www.tp1rc.edu.tw''. The main content is a table of certificates. The table has columns for 'Certificates', 'crt.sh ID', 'Logged At', 'Not Before', 'Not After', 'Matching Identities', and 'Issuer Name'. The table contains 20 rows of certificate data.

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

# Server Certificate History

\* [https://crt.sh/?CN=\\*.ntu.edu.tw](https://crt.sh/?CN=*.ntu.edu.tw)



The screenshot shows the crt.sh Identity Search interface. The search criteria are: Type: Common Name, Match: ILIKE, Search: '\*.ntu.edu.tw'. The results table lists four certificates, all issued by TWCA Secure SSL Certification Authority.

Certificates	<a href="#">crt.sh ID</a>	<a href="#">Logged At</a> ↑	<a href="#">Not Before</a>	<a href="#">Not After</a>	<a href="#">Matching Identities</a>	<a href="#">Issuer Name</a>
	<a href="#">4774242694</a>	2021-06-28	2021-06-28	2022-07-26	*.ntu.edu.tw	<a href="#">C=TW, O=TAIWAN-CA, OU=Secure SSL Sub-CA, CN=TWCA Secure SSL Certification Authority</a>
	<a href="#">1557675764</a>	2019-06-09	2019-06-04	2021-07-26	*.ntu.edu.tw	<a href="#">C=TW, O=TAIWAN-CA, OU=Secure SSL Sub-CA, CN=TWCA Secure SSL Certification Authority</a>
	<a href="#">1539909664</a>	2019-06-04	2019-06-04	2021-07-26	*.ntu.edu.tw	<a href="#">C=TW, O=TAIWAN-CA, OU=Secure SSL Sub-CA, CN=TWCA Secure SSL Certification Authority</a>
	<a href="#">26296926</a>	2016-07-29	2016-07-26	2019-07-26	*.ntu.edu.tw	<a href="#">C=TW, O=TAIWAN-CA, OU=Secure SSL Sub-CA, CN=TWCA Secure SSL Certification Authority</a>



# 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.

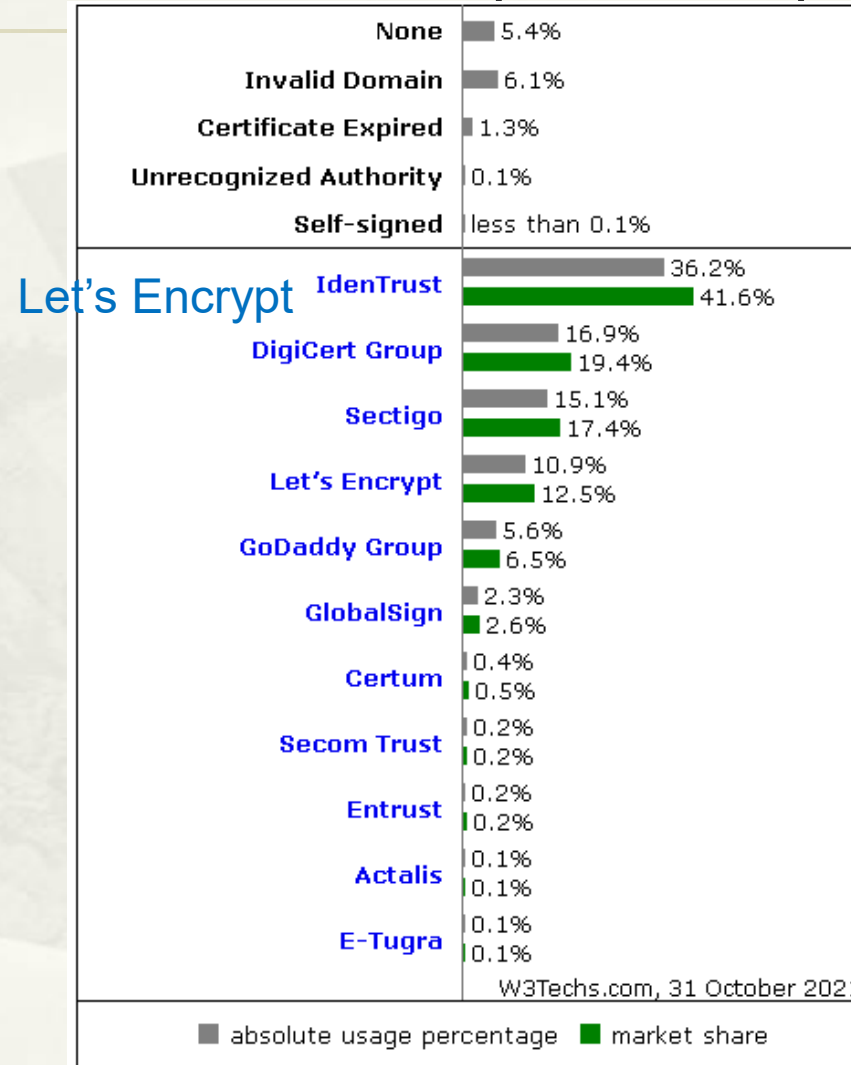
# How to Become a Trusted Certificate Authority (Public CA)

---

- \* 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.



# 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

憑證

使用目的(N): <全部>

個人 其他人 中繼憑證授權單位 受信任的根憑證授權單位 受信任的發行者 不受信任的發行者

發給	簽發者	到期日	易記名稱
Thawte Timesta...	Thawte Timestamp...	2021/1/1	Thawte Timestamp...
QuoVadis Root ...	QuoVadis Root Cer...	2021/3/18	QuoVadis Root Ce...
Microsoft Root C...	Microsoft Root Cer...	2021/5/10	Microsoft Root Cer...
<b>DST Root CA X3</b>	<b>DST Root CA X3</b>	<b>2021/9/30</b>	<b>DST Root CA X3</b>
GlobalSign	GlobalSign	2021/12/15	Google Trust Servi...
GeoTrust Global ...	GeoTrust Global CA	2022/5/21	GeoTrust Global CA
Security Commu...	Security Communica...	2023/9/30	SECOM Trust Syste...
Baltimore CyberT...	Baltimore CyberTru...	2025/5/13	DigiCert Baltimore ...
Entrust Root Cert...	Entrust Root Certifi...	2026/11/28	Entrust
Comodo CA	Comodo CA	2027/6/14	Comodo

匯入(I)... 匯出(E)... 移除(R) 進階(A)

已到期

憑證

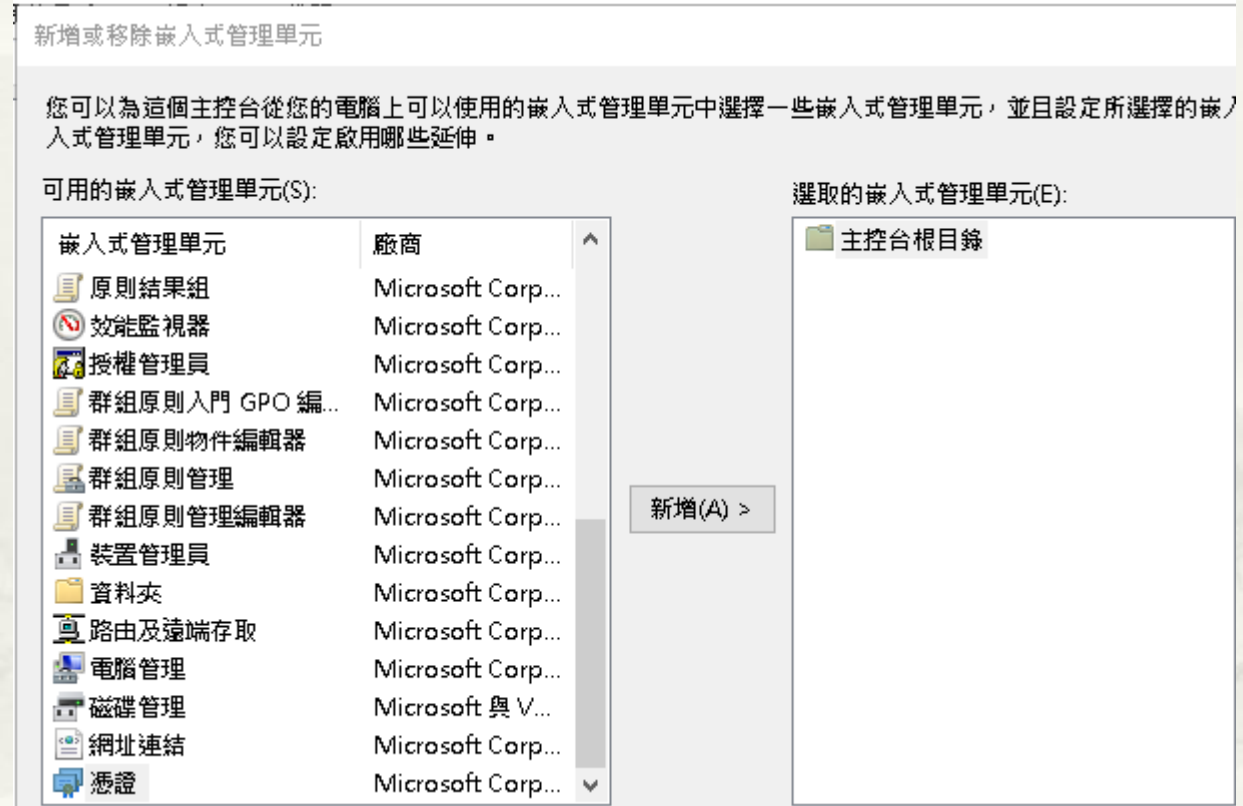
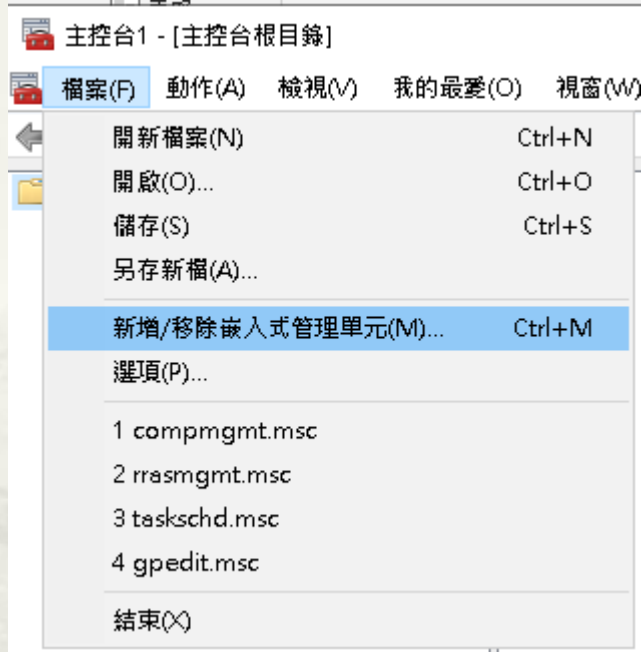
使用目的(N): <全部>

個人 其他人 中繼憑證授權單位 受信任的根憑證授權單位 受信任的發行者 不受信任的發行者

發給	簽發者	到期日	易記名稱
Microsoft Secure Server CA 2011	Microsoft Root Cer...	2026/10/19	<無>
Microsoft Windows Hardware Co...	Microsoft Root Aut...	2002/12/31	<無>
Public Certification Authority - G2	ePKI Root Certificat...	2034/12/11	<無>
<b>R3</b>	<b>ISRG Root X1</b>	<b>2025/9/16</b>	<b>&lt;無&gt;</b>
R3	DST Root CA X3	2021/9/30	<無>
RapidSSL TLS DV RSA Mixed SHA...	DigiCert Global Ro...	2023/6/1	<無>
Root Agency	Root Agency	2040/1/1	<無>
Sectigo RSA Domain Validation S...	USERTrust RSA Cer...	2031/1/1	<無>
Sectigo RSA Organization Validati...	USERTrust RSA Cer...	2031/1/1	<無>

# Root Store for Windows10

\* 開始 -> 執行: mmc



# Root Store for Windows10

## 憑證嵌入式管理單元

這個嵌入式管理單元將自動管理下列帳戶的憑證:

- 我的使用者帳戶(M)  
 服務帳戶(S)  
 電腦帳戶(C)

## 選取電腦

請選取您要此嵌入式管理單元管理的電腦。

這個嵌入式管理單元將一直管理:

- 本機電腦 (執行這個主控台的電腦)(L):  
 另一台電腦(A):    
 當電腦從命令列啟動時, 可以對這台電腦進行變更。這只有在您儲存主控台之後才適用(W)

## 新增或移除嵌入式管理單元

您可以為這個主控台從您的電腦上可以使用的嵌入式管理單元中選擇一些嵌入式管理單元, 並且設定所選擇的嵌入式管理單元。對於可延伸的嵌入式管理單元, 您可以設定啟用哪些延伸。

可用的嵌入式管理單元(S):

嵌入式管理單元	廠商
原則結果組	Microsoft Corp...
效能監視器	Microsoft Corp...
授權管理員	Microsoft Corp...
群組原則入門 GPO 編...	Microsoft Corp...
群組原則物件編輯器	Microsoft Corp...
群組原則管理	Microsoft Corp...
群組原則管理編輯器	Microsoft Corp...
裝置管理員	Microsoft Corp...
資料夾	Microsoft Corp...
路由及遠端存取	Microsoft Corp...
電腦管理	Microsoft Corp...
磁碟管理	Microsoft 與 V...
網址連結	Microsoft Corp...
憑證	Microsoft Corp...

選取的嵌入式管理單元(E):

主控台根目錄
憑證 (本機電腦)

描述:

憑證嵌入式管理單元讓您瀏覽電腦或服務的憑證存放區內容。

# Root Store for Windows10

發給	簽發者	到期日	使用目的	易記名稱
127.0.0.1	127.0.0.1	2048/4/25	伺服器驗證, 用戶端...	<無>
AAA Certificate Services	AAA Certificate Services	2029/1/1	用戶端驗證, 程式碼...	Sectigo (AAA)
Actalis Authentication Root CA	Actalis Authentication Root CA	2030/9/22	用戶端驗證, 程式碼...	Actalis Authenticat...
AddTrust External CA Root	AddTrust External CA Root	2020/5/30	用戶端驗證, 程式碼...	Sectigo (AddTrust)
AffirmTrust Commercial	AffirmTrust Commercial	2030/12/31	用戶端驗證, 程式碼...	AffirmTrust Comm...
Baltimore CyberTrust Root	Baltimore CyberTrust Root	2025/5/13	用戶端驗證, 程式碼...	DigiCert Baltimore...
Buypass Class 2 Root CA	Buypass Class 2 Root CA	2040/10/26	用戶端驗證, 加密權...	Buypass Class 2 R...
Certum CA	Certum CA	2027/6/11	用戶端驗證, 程式碼...	Certum
Certum Trusted Network CA	Certum Trusted Network CA	2029/12/31	用戶端驗證, 程式碼...	Certum Trusted N...
Changingtec ServiSign CA 20...	Changingtec ServiSign CA 2017...	2037/4/17	伺服器驗證, 用戶端...	<無>
Changingtec ServiSign CA 20...	Changingtec ServiSign CA 2017...	2037/4/17	伺服器驗證, 用戶端...	<無>
Class 3 Public Primary Certific...	Class 3 Public Primary Certificati...	2028/8/2	用戶端驗證, 程式碼...	VeriSign Class 3 P...
COMODO RSA Certification A...	COMODO RSA Certification Aut...	2038/1/19	<全部>	<無>
COMODO RSA Certification A...	COMODO RSA Certification Aut...	2038/1/19	用戶端驗證, 程式碼...	Sectigo (formerly ...
Copyright (c) 1997 Microsoft ...	Copyright (c) 1997 Microsoft C...	1999/12/31	時間戳記	Microsoft Timesta...
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	2031/11/10	用戶端驗證, 程式碼...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	2031/11/10	用戶端驗證, 程式碼...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	2038/1/15	用戶端驗證, 程式碼...	DigiCert Global R...
DigiCert High Assurance EV R...	DigiCert High Assurance EV Ro...	2031/11/10	用戶端驗證, 程式碼...	DigiCert
DigiCert Trusted Root G4	DigiCert Trusted Root G4	2038/1/15	用戶端驗證, 程式碼...	DigiCert Trusted R...
DST Root CA X3	DST Root CA X3	2021/9/30	用戶端驗證, 文件簽...	DST Root CA X3
Entrust Root Certification Aut...	Entrust Root Certification Autho...	2026/11/28	用戶端驗證, 程式碼...	Entrust





# 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's Hierarchy as of August 2021

尚未更新

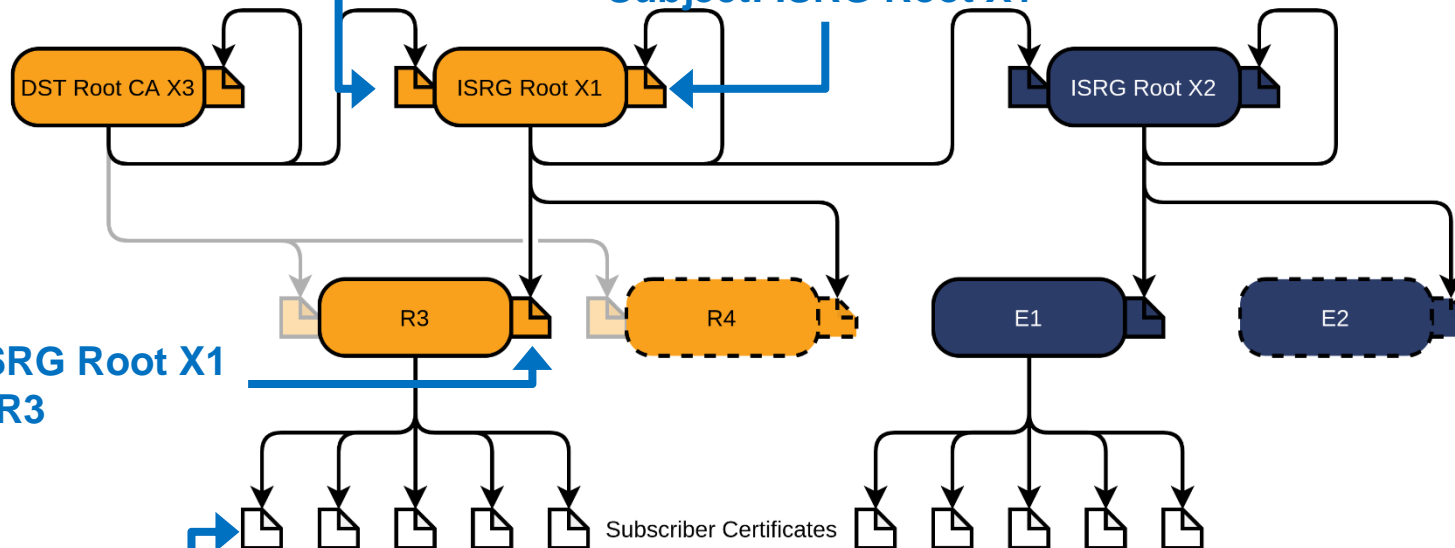
(DST Root CA X3 已是 Inactive)

Issuer: DST Root CA X3  
Subject: ISRG Root X1

Issuer: ISRG Root X1  
Subject: ISRG Root X1

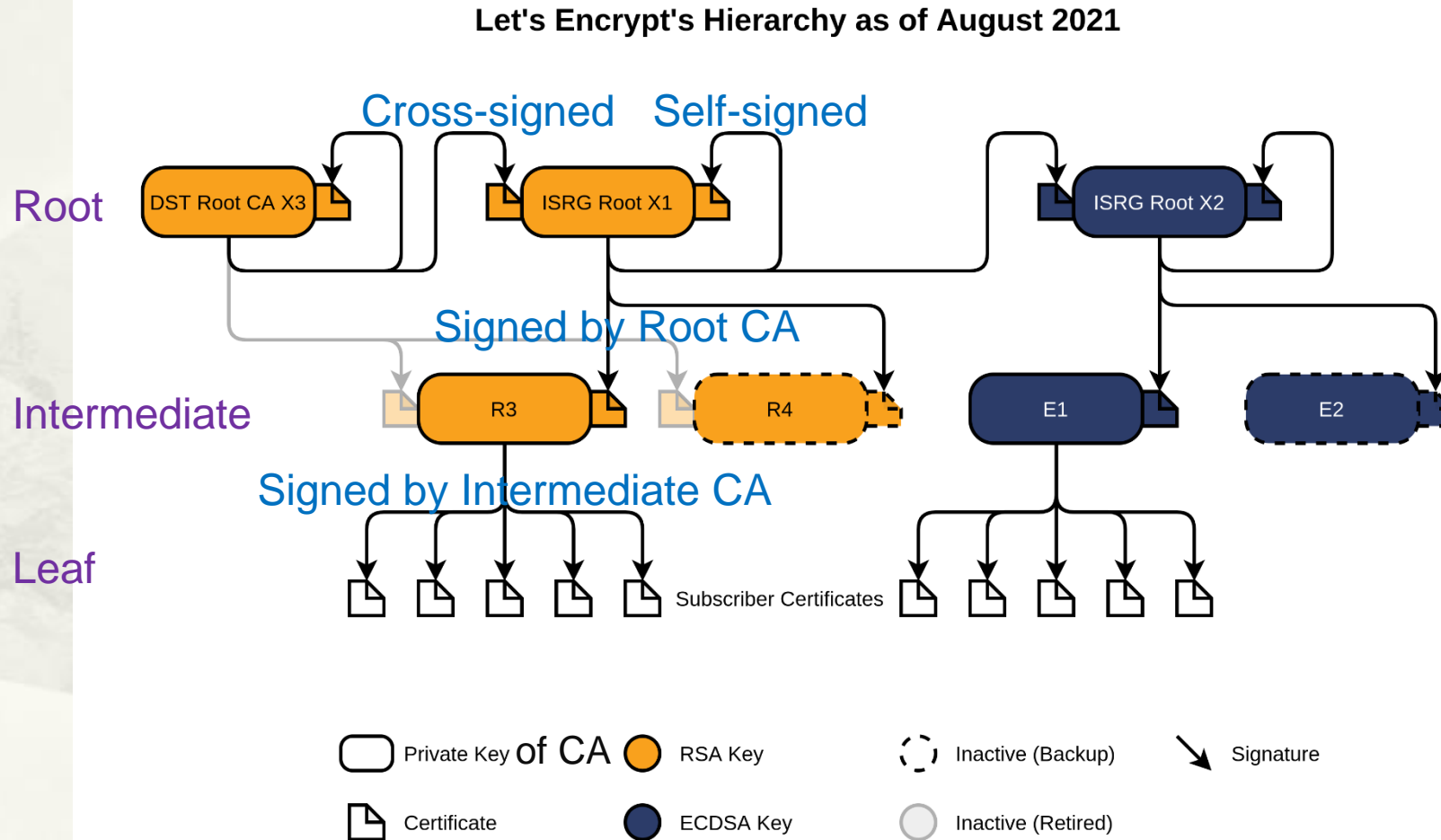
Issuer: ISRG Root X1  
Subject: R3

Issuer: R3  
Subject: www.tp1rc.edu.tw



- Private Key of CA
- RSA Key
- Inactive (Backup)
- Signature
- Certificate
- ECDSA Key
- Inactive (Retired)

# Let's Encrypt Chain of Trust



# Leaf Certificate (Server Certificate)

## CN=www.tp1rc.edu.tw

\* <https://crt.sh/?id=5372942977>

[Certificate:](#)  [Server Certificate Download \(PEM format\)](#)

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

Signed by Intermediate CA

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

效期 3個月

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:

# Intermediate CA

## CN=R3 O=Let's Encrypt

\* <https://crt.sh/?caid=183267>

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

Signed by Root  
Signed by Root  
Signed by Root

Issued Certificates	Population	Unexpired	Expired	TOTAL	Select search type:
	Certificates	237691100	479018223	716709323	IDENTITY
	Precertificates	217525340	479033265	696558605	commonName (Subject)
	TOTAL	455216440	958051488	1413267928	emailAddress (Subject)

Many

Parent CAs	<a href="#">C=US, O=Internet Security Research Group, CN=ISRG Root X1</a> <a href="#">O=Digital Signature Trust Co., CN=DST Root CA X3</a>
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 **Signed by Root CA**  
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 **效期 5年**

[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:

# Root CA

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

\* <https://crt.sh/?caid=7394>

<b>cert.sh CA ID</b>	7394																		
<b>CA Name/Key</b>	<pre>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:</pre>																		
<b>Certificates</b>	<table border="1"><thead><tr><th>cert.sh ID</th><th>Not Before</th><th>Not After</th><th>Issuer Name</th></tr></thead><tbody><tr><td><a href="#">9314791</a></td><td>2015-06-04</td><td>2035-06-04</td><td>C=US, O=Internet Security Research Group, CN=ISRG Root X1</td></tr><tr><td><a href="#">3958242236</a></td><td>2021-01-20</td><td>2024-09-30</td><td>O=Digital Signature Trust Co., CN=DST Root CA X3</td></tr></tbody></table>	cert.sh ID	Not Before	Not After	Issuer Name	<a href="#">9314791</a>	2015-06-04	2035-06-04	C=US, O=Internet Security Research Group, CN=ISRG Root X1	<a href="#">3958242236</a>	2021-01-20	2024-09-30	O=Digital Signature Trust Co., CN=DST Root CA X3						
cert.sh ID	Not Before	Not After	Issuer Name																
<a href="#">9314791</a>	2015-06-04	2035-06-04	C=US, O=Internet Security Research Group, CN=ISRG Root X1																
<a href="#">3958242236</a>	2021-01-20	2024-09-30	O=Digital Signature Trust Co., CN=DST Root CA X3																
<b>Issued Certificates</b>	<table border="1"><thead><tr><th>Population</th><th>Unexpired</th><th>Expired</th><th>TOTAL</th></tr></thead><tbody><tr><td>Certificates</td><td>5</td><td>5</td><td>10</td></tr><tr><td>Precertificates</td><td>0</td><td>0</td><td>0</td></tr><tr><td>TOTAL</td><td>5</td><td>5</td><td>10</td></tr></tbody></table>	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 <input type="text"/>
Population	Unexpired	Expired	TOTAL																
Certificates	5	5	10																
Precertificates	0	0	0																
TOTAL	5	5	10																

CA 有效日期

Self-signed  
Cross-signed

Very few

# Root CA

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

Trust	Purpose	Context (Version) <span style="color: blue;">Shortest Path</span> <span style="color: red;">Disabled From</span> <span style="color: orange;">NotBefore Until</span>									
		<a href="#">360 Browser</a> (2021-08-05)	<a href="#">Apple</a> (macOS 11.2)	<a href="#">Microsoft</a> (2021-09-10)	<a href="#">Mozilla</a> (2021-09-17)	<a href="#">Chrome</a> (2020-05-15)	<a href="#">Android</a> (2021-10-06)	<a href="#">Java</a> (16.0.1)	<a href="#">Adobe CDS</a>	<a href="#">Adobe AATL</a> (2021-09-22)	<a href="#">Adobe EUTL</a> (2021-10-01)
	Server Authentication	No	Valid <sup>1</sup>	Valid <sup>1</sup>	Valid <sup>1</sup>	Defer to OS	Valid <sup>1</sup>	Valid <sup>1</sup>	n/a	n/a	n/a
	Client Authentication	n/a	n/a	Valid <sup>1</sup>	n/a	n/a	n/a	n/a	n/a	n/a	n/a
	Secure Email	n/a	Valid <sup>1</sup>	Expired <sup>2</sup>	No	n/a	n/a	n/a	n/a	No	No
	Code Signing	n/a	Valid <sup>1</sup>	No	n/a	n/a	n/a	Valid <sup>1</sup>	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 <sup>1</sup>	Expired <sup>2</sup>	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 <sup>2</sup>	n/a	n/a	n/a	n/a	n/a	No	No
	Encrypting File System	n/a	n/a	Expired <sup>2</sup>	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 <sup>1</sup>	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
<b>Parent CAs</b>	<a href="#">O=Digital Signature Trust Co., CN=DST Root CA X3</a>										
<b>Child CAs</b>	<a href="#">C=US, O=Internet Security Research Group, CN=ISRG Root X2</a> <a href="#">C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X1</a> <a href="#">C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X2</a> <a href="#">C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3</a> <a href="#">C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X4</a> <a href="#">C=US, O=Let's Encrypt, CN=R3</a> <a href="#">C=US, O=Let's Encrypt, CN=R4</a>										

# Root Certificate CN=ISRG Root X1

\* <https://crt.sh/?id=9314791>

[Certificate:](#) → [Root Certificate Download \(PEM format\)](#)

Data:

Version: 3 (0x2)

[Serial Number:](#)

82:10:cf:b0:d2:40:e3:59:44:63:e0:bb:63:82:8b:00

Signature Algorithm: sha256WithRSAEncryption

[Issuer:](#) (CA ID: 7394)

commonName

= ISRG Root X1

organizationName

= Internet Security Research Group

countryName

= US

Validity

效期 20年

Not Before: Jun 4 11:04:38 2015 GMT

生效日 2015/06/04

Not After : Jun 4 11:04:38 2035 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:

75:c2:a2:fe:f5:6a:6e:f6:00:4f:28:db:de:68:86:

Self-signed

# 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  效期 3.5年
  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:
```

# Root CA

## CN= DST Root CA X3

\* <https://crt.sh/?caid=276>

cert.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	cert.sh ID	Not Before	Not After	Issuer Name
	<a href="#">8986898</a>	2000-09-30	2008-01-21	<a href="#">C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co., OU=DSTCA X1, CN=DST RootCA X1, emailAddress=ca@digsigtrust.com</a>
	<a href="#">8876050</a>	2004-09-08	2008-11-28	<a href="#">C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co., OU=DSTCA X1, CN=DST RootCA X1, emailAddress=ca@digsigtrust.com</a>
	<a href="#">12729827</a>	2004-09-08	2008-11-27	<a href="#">C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co., OU=DSTCA X1, CN=DST RootCA X1, emailAddress=ca@digsigtrust.com</a>
	<a href="#">8895</a>	2000-09-30	2021-09-30	<a href="#">O=Digital Signature Trust Co., CN=DST Root CA X3</a>

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)

效期 21年

Not Before: Sep 30 21:12:19 2000 GMT

Not After : Sep 30 14:01:15 2021 GMT

→ 到期日 2021/09/30

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:



# 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

## Certificate Checker

CERTIFICATE DECODER

Certificate (PEM format)

```
-----BEGIN CERTIFICATE-----  
Certificate  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
Intermediate certificate  
-----END CERTIFICATE-----
```

fullchain.pem

Check

Intermediate certificate required. Unable to get issuer certificate.

1. Subject CN: davisyoupc.cc.ntu.edu.tw > Issuer CN: R3
2. Subject CN: R3 > Issuer CN: ISRG Root X1
3. Subject CN: ISRG Root X1 > Issuer CN: DST Root CA X3

## Certificate Checker

CERTIFICATE DECODER

Certificate (PEM format)

```
-----BEGIN CERTIFICATE-----  
Certificate  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
Intermediate certificate  
-----END CERTIFICATE-----
```

fullchain\_fixed.pem

Check

No chain issues detected.

1. Subject CN: davisyoupc.cc.ntu.edu.tw > Issuer CN: R3
2. Subject CN: R3 > Issuer CN: ISRG Root X1
3. Subject CN: ISRG Root X1 > Issuer CN: ISRG Root X1

<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>

✔ Certificate Name matches incomplete-chain.badssl.com



Subject \*.badssl.com

Valid from 23/Mar/2020 to 17/May/2022

Issuer DigiCert SHA2 Secure Server CA

✘ The server is not sending the required intermediate certificate.

This server needs to be configured to include DigiCert's intermediate certificate to avoid trust errors in web browsers.

If you manage this server, you can download the file from [this link](#) or from your customer account area.

Follow the directions on [our certificate installation guide](#) to install the missing intermediate.

If you have any problems correcting this issue, please contact our helpful support team and we would be happy to assist.

\* <https://www.ssllabs.com/ssltest/analyze.html>



## Additional Certificates (if supplied)

Certificates provided 1 (1708 bytes)

Chain issues **Incomplete**

\* <https://check.twNIC.tw>

✘ trust chain of certificate

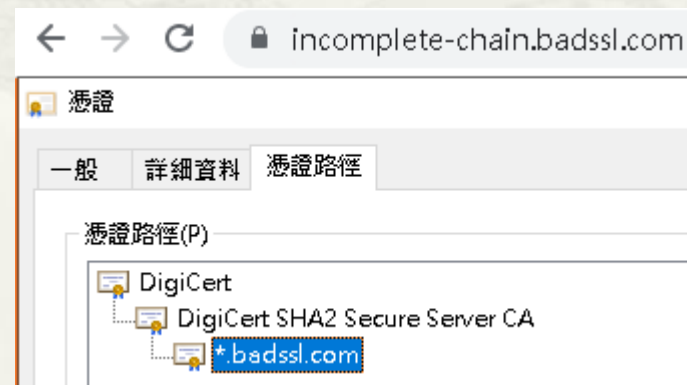
說明：


網站之憑證應由可信之CA單位簽署並且chain應完整

### Technical details:

Web server IP address	Untrusted certificate chain
104.154.89.105	*.badssl.com
-	DigiCert SHA2 Secure Server CA

\* Chrome 會自行修正



The background of the slide features a traditional Chinese landscape painting, likely a 'Shan Shui' style, rendered in a light, monochromatic tone. The painting is presented as if it were a fan, with the top edge curved and the bottom edge slightly wider, creating a semi-circular shape. The scene depicts a mountainous landscape with a winding river or path, trees, and a small structure, all rendered in fine lines and washes. The overall aesthetic is serene and classical.

# 案例: 提供錯誤 Intermediate Certificate

---



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

\* <https://www.digicert.com/help/>

✔ Certificate Name matches [www.ntub.edu.tw](https://www.ntub.edu.tw)



Subject \*.ntub.edu.tw  
Valid from 24/Feb/2021 to 24/Feb/2022  
Issuer RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1



Subject DigiCert Global Root G2  
Valid from 01/Aug/2013 to 15/Jan/2038  
Issuer DigiCert Global Root G2



Subject RapidSSL TLS RSA CA G1  
Valid from 02/Nov/2017 to 02/Nov/2027  
Issuer DigiCert Global Root G2

\* <https://www.ssllabs.com/ssltest/analyze.html>



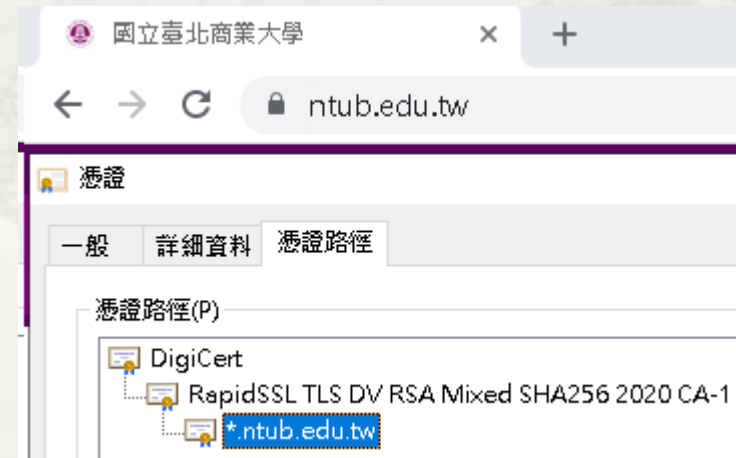
## Additional Certificates (if supplied)

Certificates provided 3 (3677 bytes)

Chain issues

Incomplete, Extra certs, Contains anchor

\* 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

Google search results for "dst root ca x3 過期". The search bar shows the query and the search button. Below the search bar, there are filters for "全部", "新聞", "圖片", "影片", "購物", and "更多". The search results show approximately 13,400 items found in 0.46 seconds.

https://blog.user.today > free-ssl-victim-dst-root-ca-x3  
**你也成為免費SSL的受害者了嗎？**  
2021年10月6日 — DST Root CA X3 根憑證過期，真的只有舊裝置會出問題？依照Let's Encrypt 的憑證信任鍊上所述，Let's Encrypt 的憑證會由DST Root CA X3 根憑證或ISRG ...

https://blog.gslin.org > archives > 2021/09/30 > dst-root-...  
**DST Root CA X3 將在今天22:01:15 過期**  
2021年9月30日 — 先前提到Let's Encrypt 發出的憑證在9/30 會產生問題，主因是IdenTrust 的 DST Root CA X3 會在9/30 過期，交叉簽名加上OpenSSL 1.0.2 的判斷條件太 ...  
您於 2021/10/28 造訪這個網頁。

https://www.linuxadictos.com > Noticias >  
**完成DST Root CA X3證書產生的問題已經開始**  
2021年10月1日 — 它在1.0.2 及以下的OpenSSL 版本和3.6.14 之前的GnuTLS 中，發生錯誤如果用於簽名的根證書之一過期，即使保留了其他有效的根證書，它也不允許正確處理交叉 ...

https://discussionschinese.apple.com > thr... > 轉為繁體網頁  
**求大神DST Root CA X3证书过期怎... - Apple 支持社区**  
2021年10月8日 — 也就是工作用，主要是为了出差方便。但现在浏览器显示DST Root CA X3根证书过期了，有解决方法吗？  
6 個答案 · 最佳解答：主要是不確定這個證書是什麼時候更新的，建議預約 Apple store 逐版本的...

- \* 2020/05/30，串流製造商Roku、支付業者Stripe與Spredly、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>

iThome news article titled "根憑證過期造成Roku、Stripe及Spredly等眾多服務停擺，專家預期更多案例將接踵而來". The article is dated 2020-06-12 and has 6.7 million views. The author is 陳曉莉. The article discusses the expiration of the DST Root CA X3 certificate and its impact on various services.

根憑證過期造成Roku、Stripe及Spredly等眾多服務停擺，專家預期更多案例將接踵而來

資安專家警告，未來幾年將有更多根憑證陸續到期，恐波及各種連網服務或裝置，其中包括明年9月底過期的IdenTrust DST Root CA X3

文/ 陳曉莉 | 2020-06-12 發表

6.7 萬 按讚加入iThome粉絲團 409 分享

# SSL 數位憑證審判日

\* <https://letsencrypt.org/docs/certificate-compatibility/>

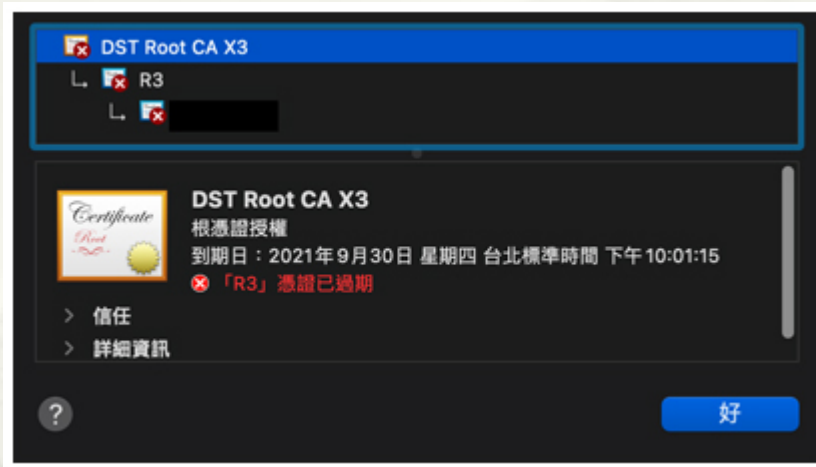
## Platforms that trust DST Root CA X3 but not ISRG Root X1

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

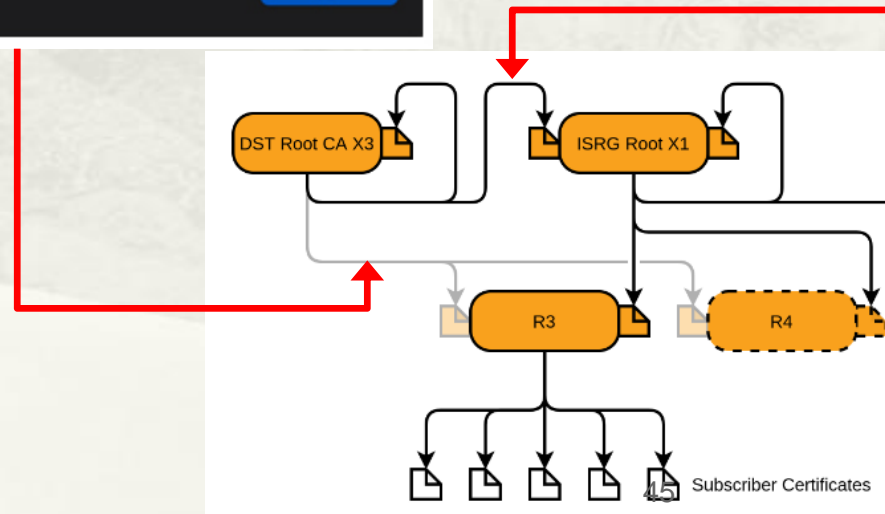
- macOS < 10.12.1
- iOS < 10
- Mozilla Firefox < 50
- Ubuntu >= intrepid / 8.10
- Debian >= squeeze / 6 and < jessie / 8
- Java 8 >= 8u101 and < 8u141
- Java 7 >= 7u111 and < 7u151
- NSS >= v3.11.9 and < 3.26
- Amazon FireOS (Silk Browser) (version range unknown)
- Cyanogen > v10 (version that added 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







# 案例: Root Certificate Cross-signed With Expired CA

---

# letsencrypt.org

\* <https://www.digicert.com/help>

✔ Certificate Name matches letsencrypt.org



Subject lencr.org  
Valid from 10/Oct/2021 to 08/Jan/2022  
Issuer R3



Subject R3  
Valid from 04/Sep/2020 to 15/Sep/2025  
Issuer ISRG Root X1



Subject ISRG Root X1  
Valid from 20/Jan/2021 to 30/Sep/2024  
Issuer DST Root CA X3

\* <https://check.twnic.tw/>

## Certificate

✘ trust chain of certificate

說明：

網站之憑證應由可信之CA單位簽署並且chain應完整

### Technical details:

Web server IP address	Untrusted certificate chain
2406:da18:880:3802:bc32:fc44:302b:aad2	lencr.org
-	R3
178.128.104.229	lencr.org
-	R3

\* Chrome



Root Certificate 不相同

發給: ISRG Root X1  
簽發者: ISRG Root X1



# 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](http://www.hcrc.edu.tw)
- \* 台大區網 (已修正)
  - \* [www.tp1rc.edu.tw](http://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