

HTTPS 憑證簽署架構

Certificate Chain

臺灣大學計資中心

網路組

游子興

大綱

- * Certificate Chain
- * Certificate Chain Problems
- * How to Fix Certificate Chain Problems

The background of the slide is a light beige color. In the center, there is a large, semi-circular graphic that resembles a traditional Chinese folding fan. The fan is open, showing a landscape painting in a traditional Chinese style. The painting depicts mountains, trees, and a body of water. The colors are muted, with shades of green, brown, and grey. The fan's ribs are visible, creating a radial pattern. The title "Certificate Chain" is centered over the fan.

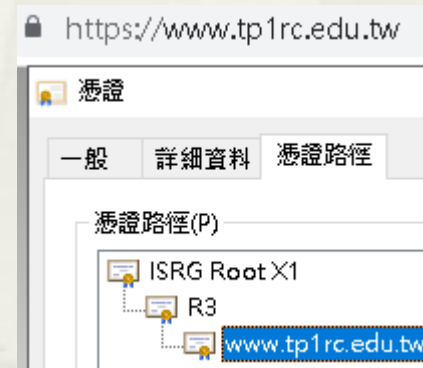
Certificate Chain

Certificate Chain Example

* www.ntu.edu.tw



* www.tp1rc.edu.tw



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, Line API) 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。
- * Best Practice
 - * Server should always send a complete trust chain. The trust chain contains your certificate concatenated with all intermediate certificates.

Let's Encrypt Chain of Trust

<https://letsencrypt.org/certificates/>

Let's Encrypt's Hierarchy as of August 2021

尚未更新

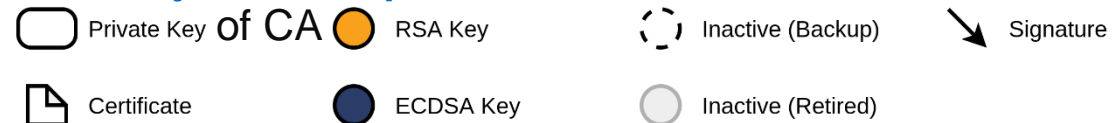
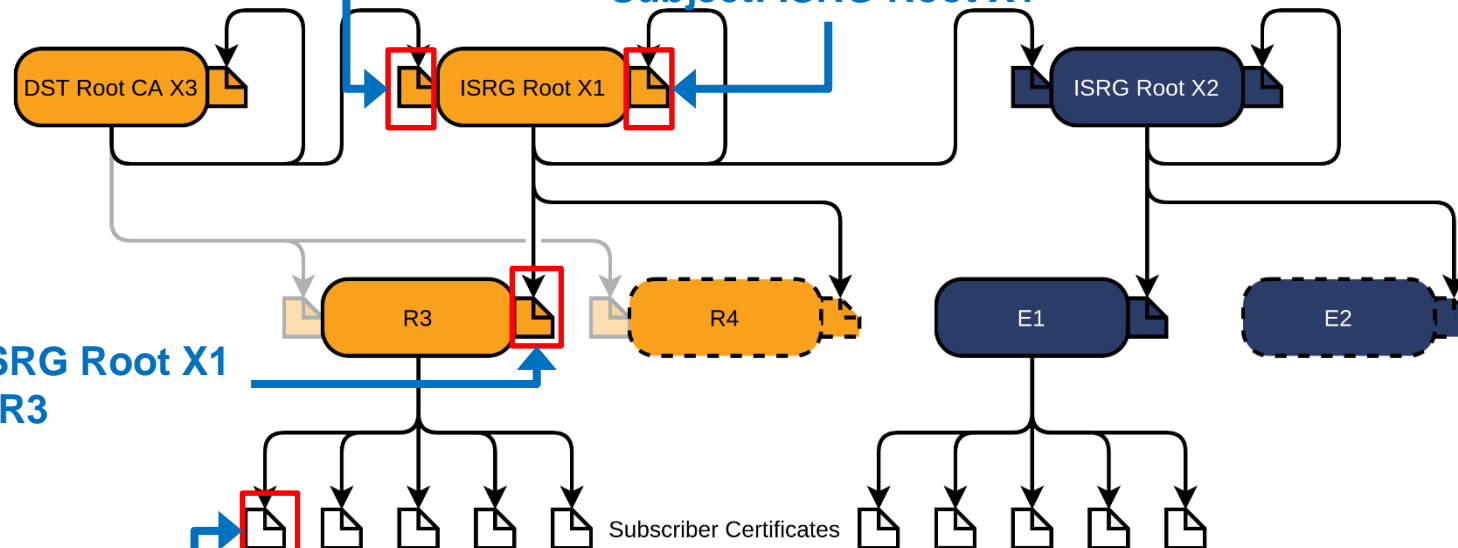
(DST Root CA X3 已是 Inactive)

Issuer: DST Root CA X3
Subject: ISRG Root X1

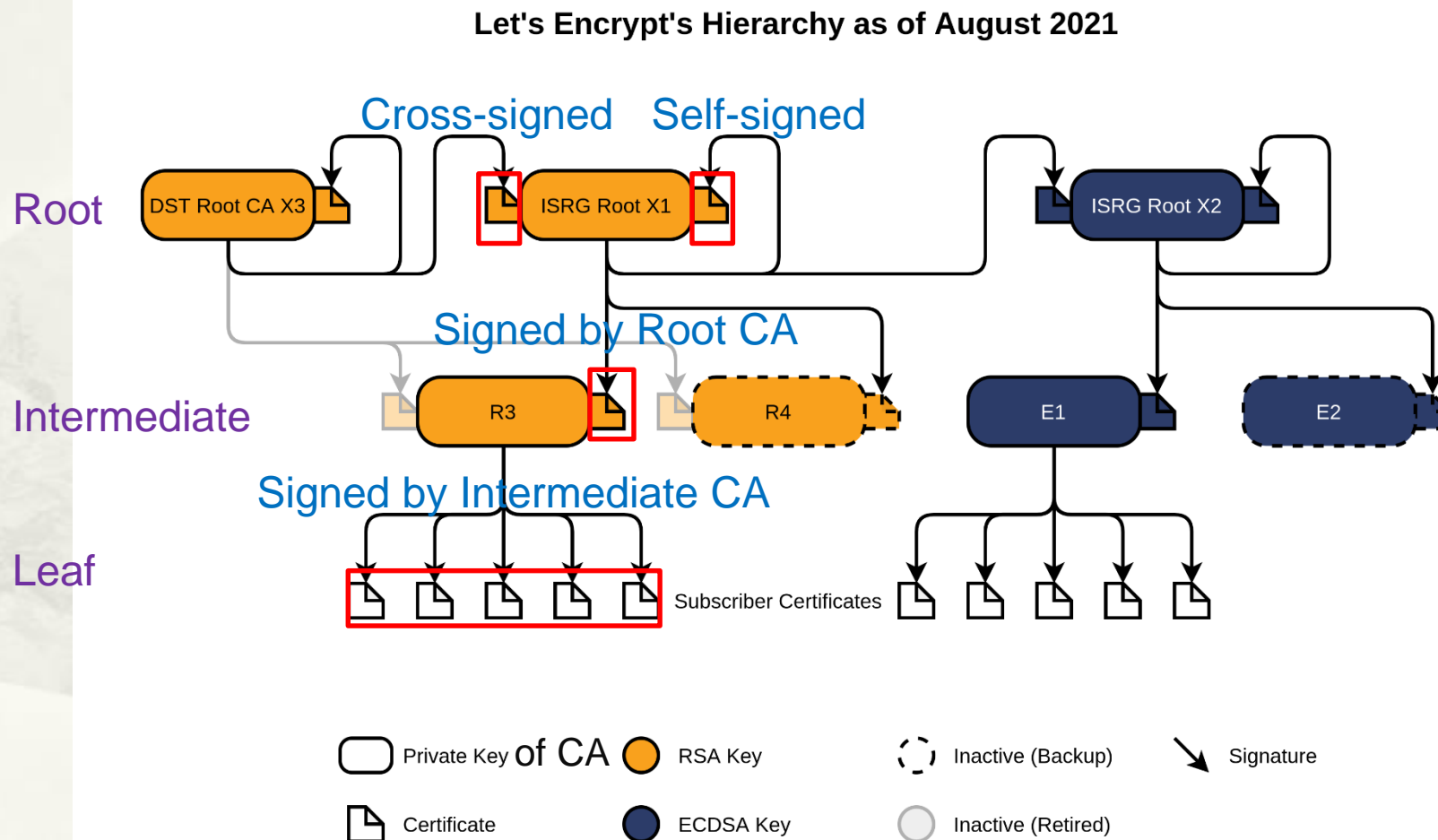
Issuer: ISRG Root X1
Subject: ISRG Root X1

Issuer: ISRG Root X1
Subject: R3

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



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>

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

Signed by Root CA

organizationName = Internet Security Research Group

countryName = US

Validity

Not Before: Sep 4 00:00:00 2020 GMT

效期 5年

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:

Root CA

CN=ISRG Root X1 (1/2)

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

cert.sh CA ID	7394			
CA Name/Key	<div>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:</div>			
Certificates	cert.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
Issued Certificates	Population	Unexpired	Expired	TOTAL
	Certificates	5	5	10
	Precertificates	0	0	0
	TOTAL	5	5	10
Select search type:		Enter search text (% = All certificates)		
IDENTITY				
commonName (Subject)				
emailAddress (Subject)				

CA 有效日期

Self-signed
Cross-signed

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>

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

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

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

效期 20年

生效日 2015/06/04

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>

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
	8876050	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
	8895	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)

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 Check

* Online Service

- * <https://www.ssllabs.com/ssltest/analyze.html>
- * <https://www.digicert.com/help/>
- * <https://ssltools.godaddy.com/views/certChecker>
- * <https://www.sslchecker.com/sslchecker> (有時怪怪的)
- * <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**

僅提供自身 Server Certificate

未提供 Intermediate Certificate

Test Site: incomplete-chain.badssl.com

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

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

✓ 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.

✗ 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

104.154.89.105

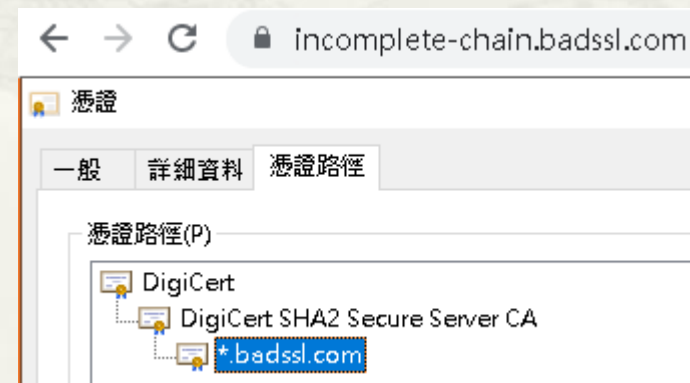
-

Untrusted certificate chain

*.badssl.com

DigiCert SHA2 Secure Server CA

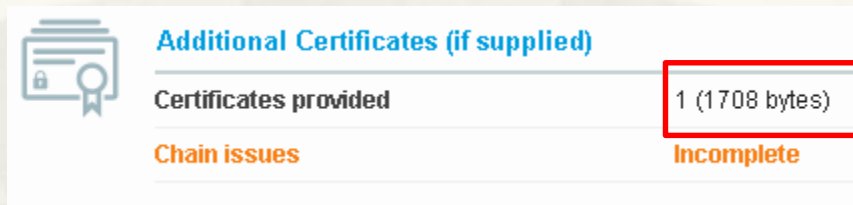
* Chrome 會自行修正



未提供 Intermediate Certificate

Test Site: incomplete-chain.badssl.com

* <https://www.ssllabs.com/ssltest/analyze.html?d=incomplete-chain.badssl.com>

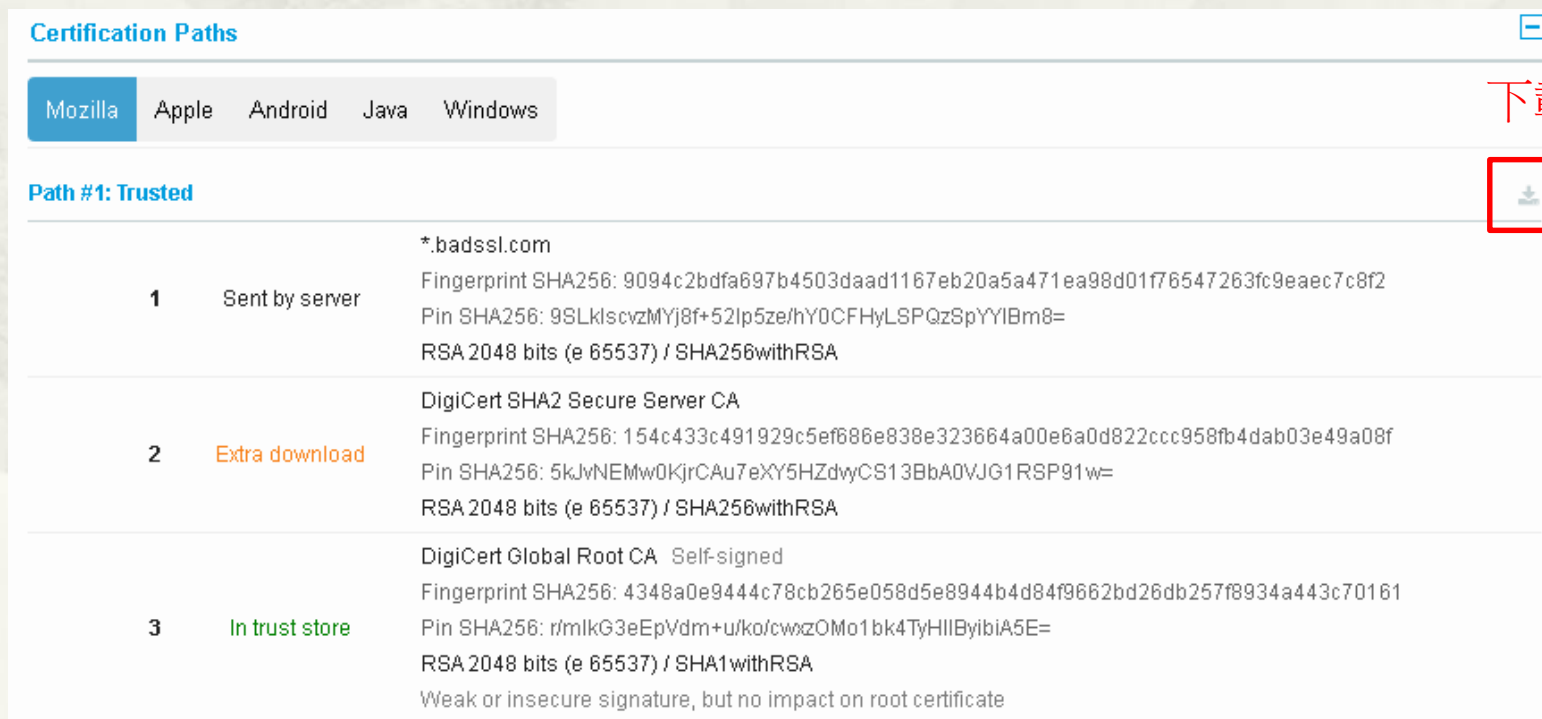


Additional Certificates (if supplied)

Certificates provided	1 (1708 bytes)
Chain issues	Incomplete

僅提供自身 Server Certificate

* 修正後 Certificate Chain



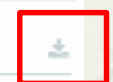
Certification Paths

Mozilla Apple Android Java Windows

Path #1: Trusted

1	Sent by server	*.badssl.com Fingerprint SHA256: 9094c2bd6a697b4503daad1167eb20a5a471ea98d01f76547263fc9eaec7c8f2 Pin SHA256: 9SLklscvzMYj8f+52lp5ze/hY0CFHyLSPQzSpYYIBm8= RSA 2048 bits (e 65537) / SHA256withRSA
2	Extra download	DigiCert SHA2 Secure Server CA Fingerprint SHA256: 154c433c491929c5ef686e838e323664a00e6a0d822ccc958fb4dab03e49a08f Pin SHA256: 5kJvNEMw0KjrCAu7eXY5HZdwyCS13BbA0VJG1RSP91w= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	DigiCert Global Root CA Self-signed Fingerprint SHA256: 4348a0e9444c78cb265e058d5e8944b4d84f9662bd26db257f8934a443c70161 Pin SHA256: r/mlkG3eEpVdm+u/ko/cwXzOMo1bk4TyHIIByibiA5E= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

下載



The background of the slide features a traditional Chinese landscape painting, likely a 'Shan Shui' (mountain-water) genre, rendered on a fan. The painting depicts a misty, mountainous landscape with a winding path or river, and is characterized by fine ink lines and a soft, atmospheric quality. The fan is positioned centrally, with its handle at the bottom and the painted surface fanning out towards the top.

案例：提供錯誤 Intermediate Certificate

提供錯誤 Intermediate Certificate

Test Site: www.ntub.edu.tw

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

* Chrome 會自行修正

✔ Certificate Name matches 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

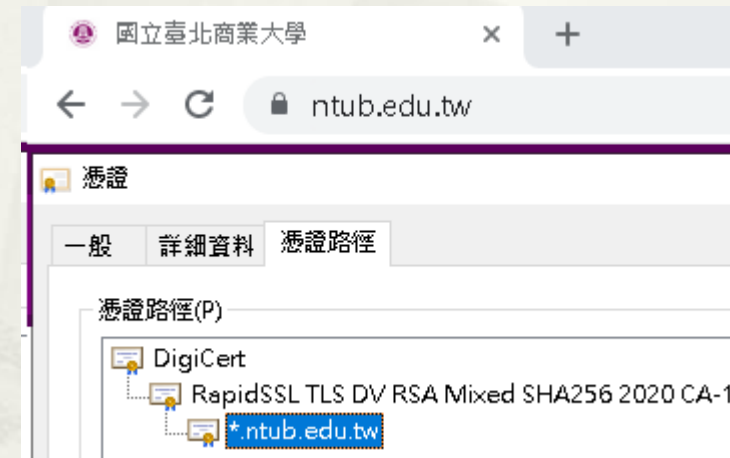


Root Certificate



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


Intermediate Certificate



提供錯誤 Intermediate Certificate

Test Site: www.ntub.edu.tw

* <https://www.ssllabs.com/ssltest/analyze.html?d=www.ntub.edu.tw>



Additional Certificates (if supplied)
Certificates provided 3 (3677 bytes) 提供 3 Certificates
Chain issues Incomplete, Extra certs, Contains anchor

* 修正後 Certificate Chain

Certification Paths

Mozilla Apple Android Java Windows

Path #1: Trusted

1

Sent by server

*.ntub.edu.tw
Fingerprint SHA256: 515b0d045dbdb6477725a255e03987cb49f6ca1be2878f3790600d8cad5c0208
Pin SHA256: oREbcQnH5pw4AQhCIKinQ/qcIF2wzru0ApTEdzKRwZE=
RSA 2048 bits (e 65537) / SHA256withRSA

2

Extra download

RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1
Fingerprint SHA256: e6fa484a858940d101978555454aa466531ab6c4abc4ad2b000626aaac0d04f9
Pin SHA256: 48hXNwn3IaJAzsrIBprOcewUb097BGNL7e+MVM7Rcis=
RSA 2048 bits (e 65537) / SHA256withRSA

3

In trust store

DigiCert Global Root CA Self-signed
Fingerprint SHA256: 4348a0e9444c78cb265e058d5e8944b4d84f9662bd26db257f8934a443c70161
Pin SHA256: r/mlkG3eEpVdm+u/ko/cwøzOMo1bk4TyHlIByibiA5E=
RSA 2048 bits (e 65537) / SHA1withRSA
Weak or insecure signature, but no impact on root certificate

下載



案例: **Root Certificate** 過期

根憑證到期日 ≈ SSL 數位憑證審判日

* 2021/09/30 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 number of results (13,400). The first result is from <https://blog.user.today> with the title "你也成為免費SSL的受害者了嗎?". The second result is from <https://blog.gslin.org> with the title "DST Root CA X3 將在今天22:01:15 過期". The third result is from <https://www.linuxadictos.com> with the title "完成DST Root CA X3證書產生的問題已經開始". The fourth result is from <https://discussionschinese.apple.com> with the title "求大神DST Root CA X3证书过期怎... - Apple 支持社区".

* 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 discusses the expiration of the DST Root CA X3 certificate and its impact on various services. It includes a sub-headline "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". The article is dated 2020-06-12 and has 6.7K likes and 409 shares.

SSL 數位憑證審判日

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

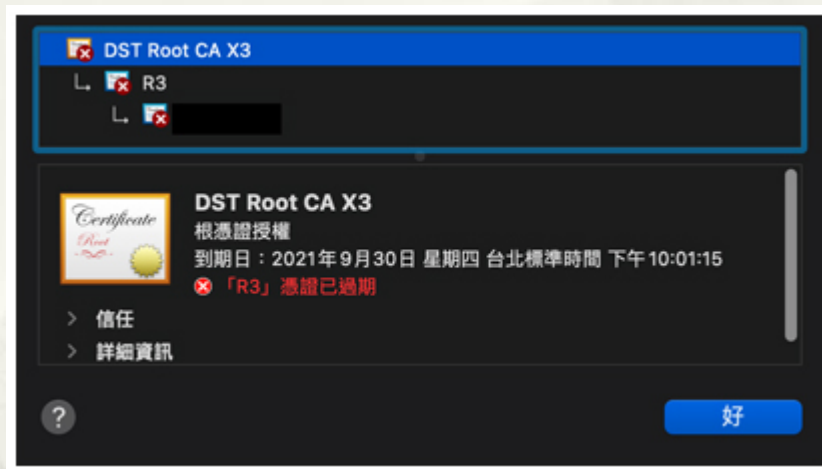
Platforms that trust DST Root CA X3 but not ISRG Root X1

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

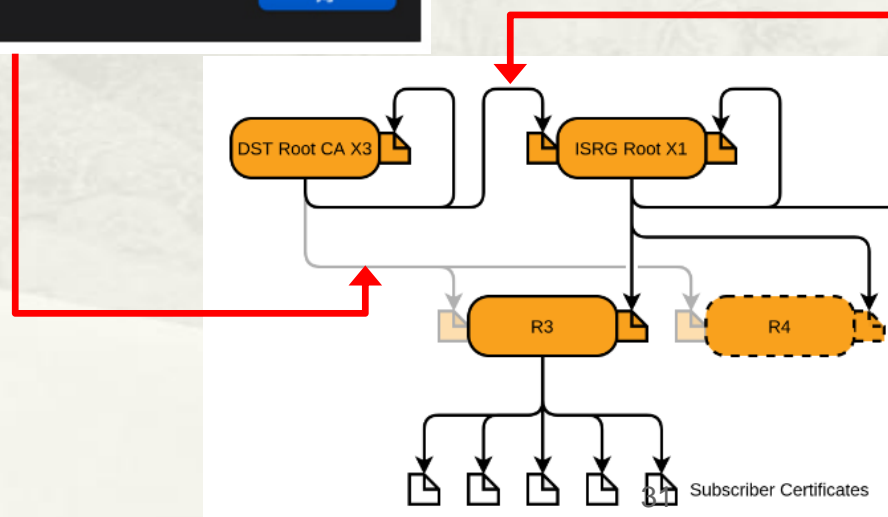
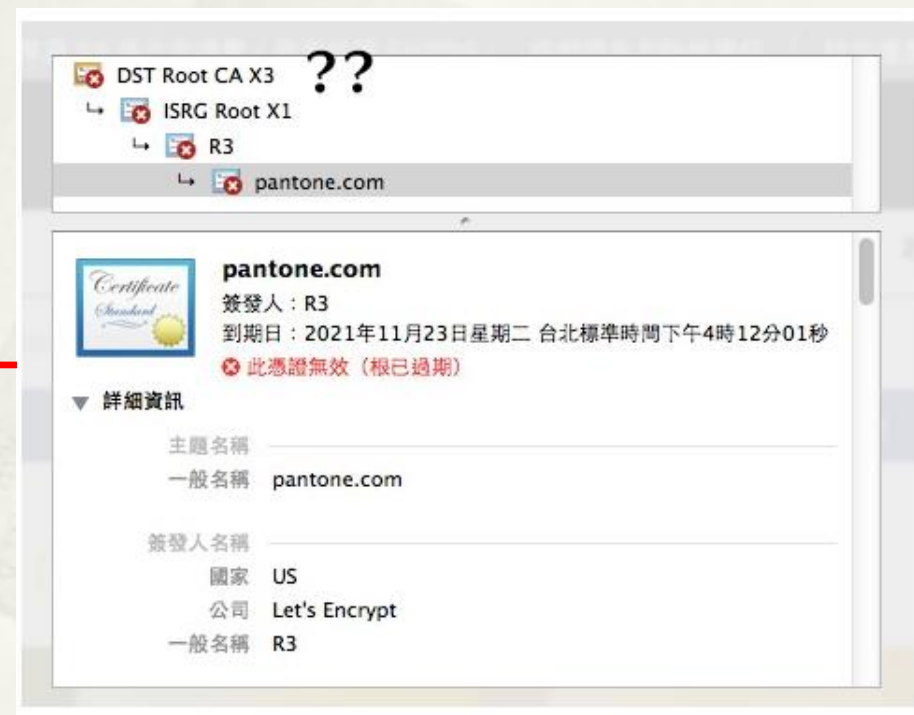
- macOS < 10.12.1
- iOS < 10
- Mozilla Firefox < 50
- Ubuntu >= intrepid / 8.10
- Debian >= squeeze / 6 and < jessie / 8
- Java 8 >= 8u101 and < 8u141
- Java 7 >= 7u111 and < 7u151
- NSS >= v3.11.9 and < 3.26
- Amazon FireOS (Silk Browser) (version range unknown)
- Cyanogen > v10 (version that added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



體驗 SSL 數位憑證審判日

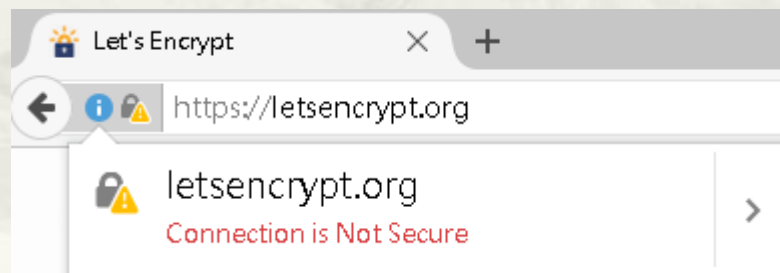
使用舊版 Firefox 49

- * Firefox 49 下載

- * <https://ftp.mozilla.org/pub/firefox/releases/49.0/win64/en-US/>

- * 連線顯示不安全

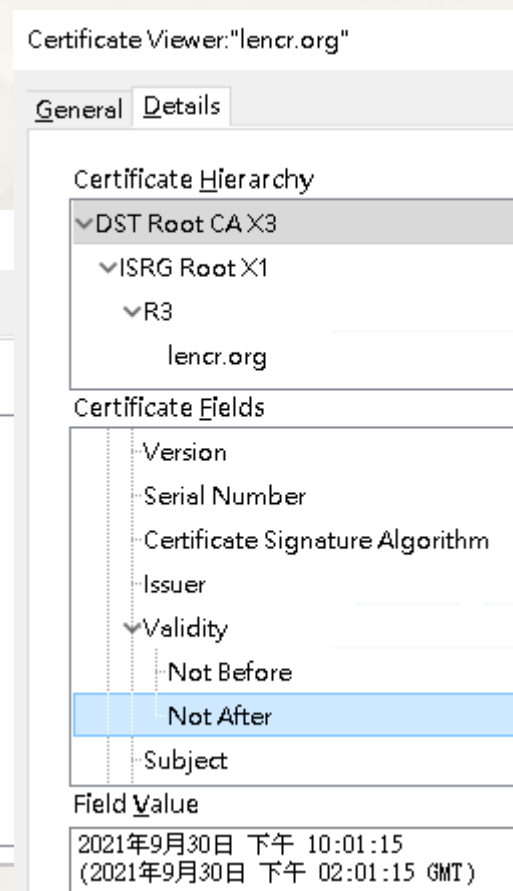
- * <https://letsencrypt.org/>



- * 原因: 未包含 ISRG Root X1 根憑證



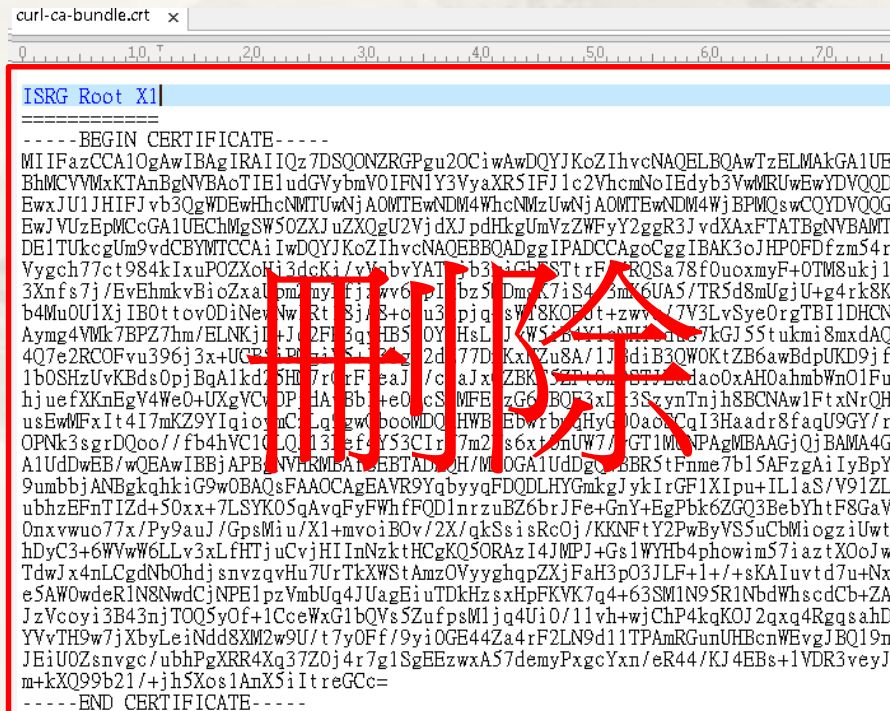
未包含 ISRG Root X1



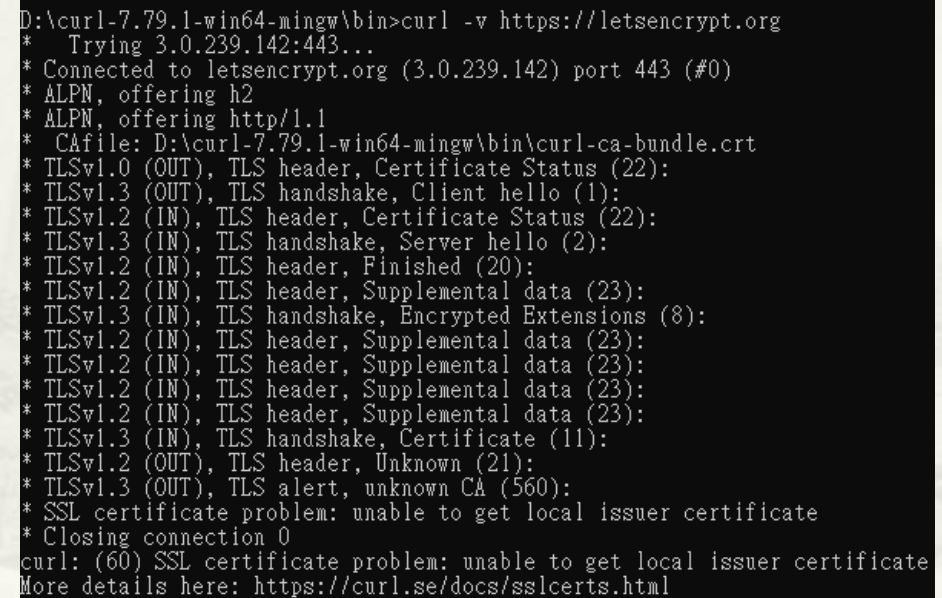
根憑證已過期

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



```
curl-ca-bundle.crt x
-----BEGIN CERTIFICATE-----
MIIFAzCCA1OgAwIBAgIRAIQz7DSQONZRGpGu20CiwAwDQYJKoZIhvcNAQELBQAwTzELMAkGA1UE
BhMCVVMKTAAnBgNVBAAoTIEludG9ybmV0IFN1Y3VyaXR5IFJlc2VhcnNoIEdyb3VwMRUwEwYDVQOQ
EwJUU1JHIFJvb3QgWDEwHhcNMjUwNjA0MTEwNDM4WWhcNMzUwNjA0MTEwNDM4WjBPMQswCQYDVQOQ
EwJVUzEpMjUwNjA0MTEwNDM4WjBPMQswCQYDVQOQDElTUkcgUm9vdCBYMTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAK3oJHP0FDfzm54r
Vygch77ct984kIxuPOZxOfi3dcKi/vYabvYATtgb3iGfSTtrF/RQSa78f0uoxmyF+OTM8ukj1
3Xnfs7j/EvEhmkvBioZxalpmmyEjwv6p1bz5DmsK7iS43mX6UA5/TR5d8mUgjU+g4rk8K
b4MuOU1XjIB0ttov0DiNeNwRt8j/3+c3piqsW18KOFdt+zwv/7V3LvSyeOrgTBI1DHcn
Aymg4VMk7BPZ7hm/ELNkj1+J2F8qgHB5OYHsLJW524V1NMTd837kGJ55tukmi8mxdAQ
4Q7e2RCOFvu396j3x+UCR6P83S3z2d77DKXZu8A/1JbdiB3QWOKtZB6awBdpUKD9jf
1b0SHzUvKBdsOpjBqA1kd5H7r0rF8aJ/caxZBK5Z2P6aETJ2adac0xAH0ahmbWn01Fu
hjuefXKnEgV4We0+UXgYVCOPdABbje0cSMFEzG6BQF3xL3SzynTnjh8BCNAw1FtxNrQH
usEwMFxlt4I7mKZ9YIqioacCqgzw0oowMDQHWBEBwrbqHyG00aocQqI3Haadr8faqU9GY/r
OPNk3sgrDQoo//fb4hVC1CQ131efY53CIR7m2s6xt0nUW7/1GT1MNPAGMBAAGjQjBAMAAG
A1UdDwEB/wQEAwIBBjAPBjwVhRMbA1EBBTABJH/MOGA1UdDgQ1BR5tFnme7b15AFzgAiIyBpY
9umbbjANBgkqhkiG9w0BAQsFAAOCAgEAVR9YqbyyqFDQDLHYGmkGjykIrGF1XIpu+IL1aS/V91ZL
ubhzEFnTIZd+50xx+7LSYK05qAvqFyFWHfFQD1nrzuBZ6brJFe+GnY+EgPbk6ZGQ3BebYhtF8GaV
Onxvwuo77x/Py9auJ/GpsMiu/X1+mvoiBOv/2X/gkSsisRcOj/KKNftY2PwByVS5uCbMiozgiUwt
hDyC3+6WYwW6LLv3xLHFTUcVjHIInNzktHCgKQ50RAZi4JMPJ+Gs1WYHb4phowim57iazTX0oJw
TdwJx4nLCgdNbOhndjsnvzqVHu7UrTkXWStAmzOVyyghqpZXjFaH3pO3JLE+1/+sKAiuvtd7u+Nx
e5AWOwdeR1N8NwdCjNPE1pzVmbUq4JUagEiUTDkHszxHPfKVK7q4+63SM1N95R1NbdWhscdCb+ZA
JzVcoyi3B43njTOQ5yOf+1CceWxG1bQVs5ZufpsW1jq4Ui0/11vh+wjChP4kqKOJ2qxq4RgqsahD
YVvTH9w7jXbyLeiNdd8XM2w9U/t7yOf/9yi0GE44Za4rF2LN9d11TPAmRGunUHBcnWBEvgJBQ19n
JEiUOZsnvgc/ubhPgXRR4Xq37Z0j4r7g1SgBEzwxA57demyPxgcYxn/eR44/KJ4EBs+1VDR3veyJ
m+kXQ99b21/+jh5Xos1AnXSiItrEGCc=
-----END CERTIFICATE-----
```



```
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

Root Certificate Cross-signed With Expired CA

Test Site: 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:

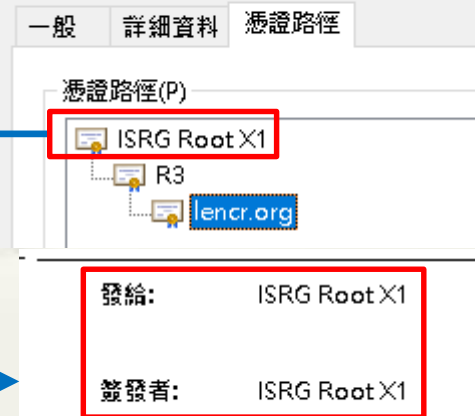
Web server IP address

2406:da18:880:3802:bc32:fc44:302b:aad2
-
178.128.104.229
-

Untrusted certificate chain

lencr.org
R3
lencr.org
R3

* Chrome



Root Certificate 不相同

Root Certificate Cross-signed With Expired CA

Test Site: letsencrypt.org

- * <https://www.ssllabs.com/ssltest/analyze.html?d=letsencrypt.org>

Additional Certificates (if supplied)

Certificates provided	3 (3881 bytes)
Chain issues	None

- * 修正後 Certificate Chain

Certification Paths		
Mozilla Apple Android Java Windows		
Path #1: Trusted		
1	Sent by server	lencr.org Fingerprint SHA256: d353c3ef9e6bfa93d4d8df09ecc625f5d2199014d97727f29b5f3df9524bcfdb Pin SHA256: vPAsw8+5GrAkQqC5zMfST4GbVSLEShowOeWw7+GAnA= EC 256 bits / SHA256withRSA
2	Sent by server	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTb1h0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	ISRG Root X1 Self-signed Fingerprint SHA256: 96bce06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6 Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA

- * 網站提供 Certificate Chain

Path #2: Not trusted (invalid certificate [Fingerprint SHA256: 0687260331a72403d909f105e69bcf0d32e1bd2493ffc6d9206d11bcd6770739])		
1	Sent by server	lencr.org Fingerprint SHA256: d353c3ef9e6bfa93d4d8df09ecc625f5d2199014d97727f29b5f3df9524bcfdb Pin SHA256: vPAsw8+5GrAkQqC5zMfST4GbVSLEShowOeWw7+GAnA= EC 256 bits / SHA256withRSA
2	Sent by server	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTb1h0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0= RSA 2048 bits (e 65537) / SHA256withRSA
3	Sent by server	ISRG Root X1 Fingerprint SHA256: 6d99fb265eb1c5b3744765fcbcb648f3cd8e1bffa4dc4c2f99b9d47cf7ff1c24f Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA
4	In trust store	DST Root CAX3 Self-signed Fingerprint SHA256: 0687260331a72403d909f105e69bcf0d32e1bd2493ffc6d9206d11bcd6770739 Pin SHA256: Vjs8r4z+80wjNcr1YKpVWQboSIRi63WwXhIMN+eWys= RSA 2048 bits (e 65537) / SHA1withRSA Valid until: Thu, 30 Sep 2021 14:01:15 UTC EXPIRED Weak or insecure signature, but no impact on root certificate

建議使用: ISRG Root X1(Self-singed)

Root Certificate Cross-signed With Expired CA

Test Site: letsencrypt.org

* <https://www.sslchecker.com/sslchecker>

* 自行測試

CERTIFICATE CHAIN

YOUR CERT
found
DOWNLOAD

CHAIN CERT 1
found
DOWNLOAD

CHAIN CERT 2
found
DOWNLOAD

ROOT 1
missing
DOWNLOAD

CHAIN DETAILS ? < Hide

Issuer R3	Issuer ISRG Root X1	Issuer DST Root CA X3	Issuer NA
Common name lencr.org	Common name R3	Common name ISRG Root X1	Common name DST Root CA X3
Organization NA	Organization Let's Encrypt	Organization Internet Security Research Group	Organization Digital Signature Trust Co.
Issued Oct 10, 2021	Issued Sep 04, 2020	Issued Jan 20, 2021	Issued Sep 30, 2000
Expires Jan 08, 2022	Expires Sep 15, 2025	Expires Sep 30, 2024	Expires Sep 30, 2021

憑證

一般 詳細資料 憑證路徑

憑證資訊

這個憑證已到期或尚未生效。

發給: ISRG Root X1

簽發者: DST Root CA X3

有效期自 2021/1/21 到 2024/10/1

憑證

一般 詳細資料 憑證路徑

憑證路徑(P)

DST Root CA X3
ISRG Root X1

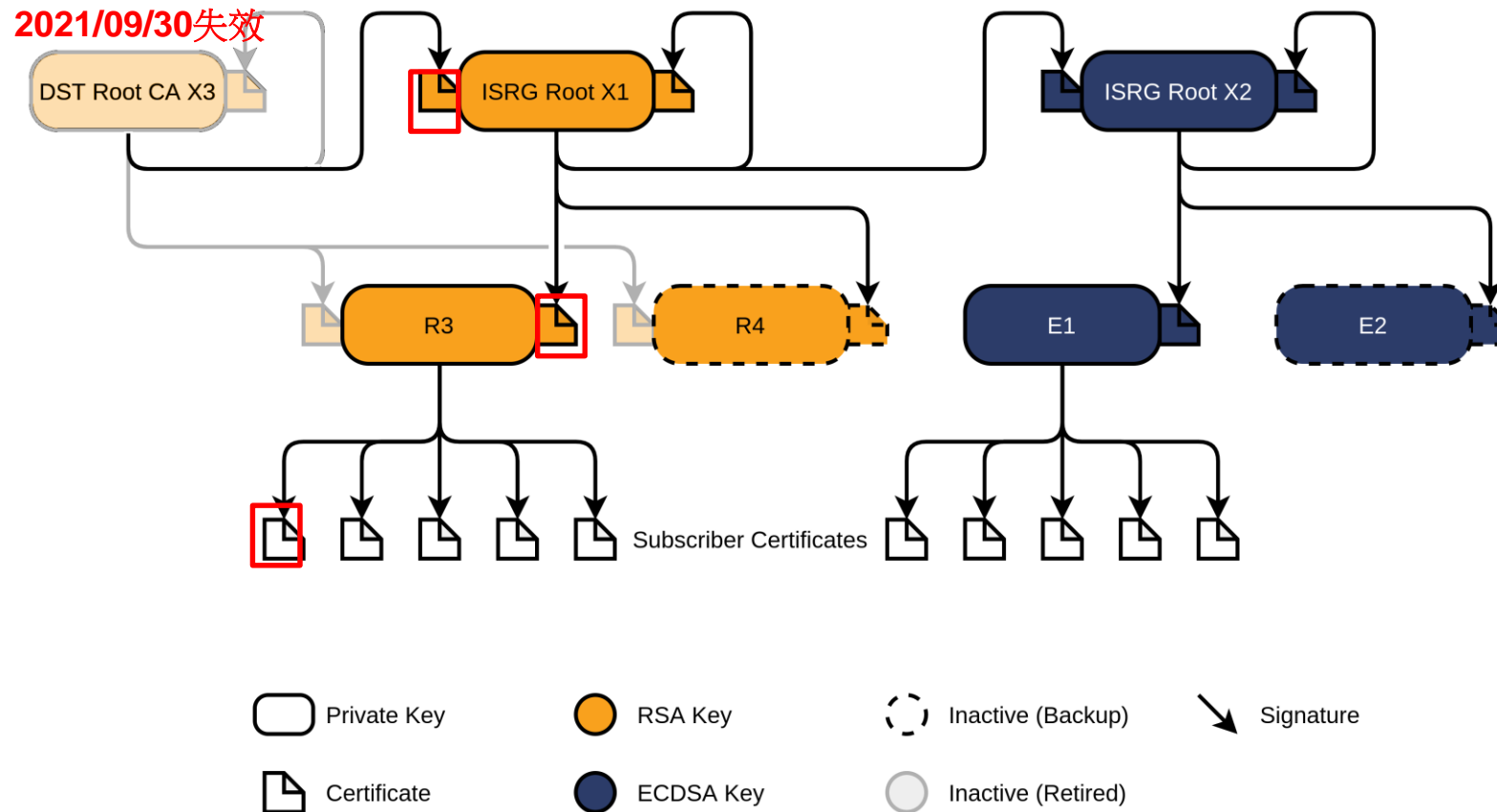
憑證狀態(S):

這個憑證已到期或尚未生效。

Root Certificate Cross-signed With Expired CA

Test Site: letsencrypt.org

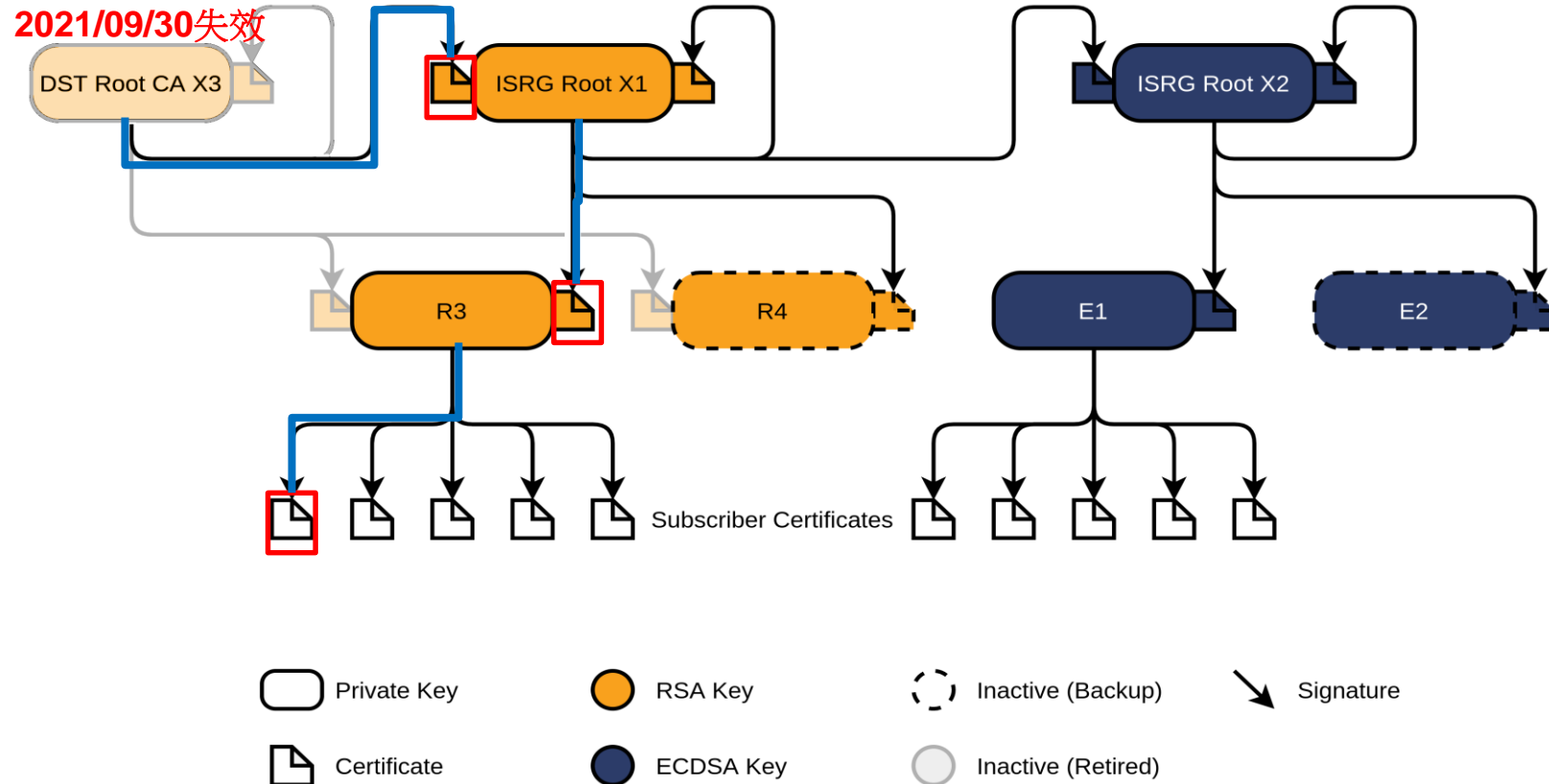
Let's Encrypt's Hierarchy as of August 2021



Root Certificate Cross-signed With Expired CA

Test Site: letsencrypt.org

Let's Encrypt's Hierarchy as of August 2021



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

The background of the slide features a large, semi-circular graphic that resembles a traditional Chinese landscape painting, such as a 'Shan Shui' (mountain-water) scene. This graphic is rendered in a light, monochromatic style and is set against a light beige background. The painting depicts a mountainous landscape with a winding river or path, and is divided into several vertical panels, similar to a folding fan. The title text is centered over this graphic.

案例: **Extra Root Certificate**


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.

Extra Root Certificate

Test Site: www.tp1rc.edu.tw

- * <https://www.ssllabs.com/ssltest/analyze.html?d=www.tp1rc.edu.tw>

 Additional Certificates (if supplied)	
Certificates provided	3 (4017 bytes)
Chain issues	Contains anchor

- * Add Intermediate as well as Root CA
- * Only need the Intermediate as the client will already have Root CA.
 - * <https://success.qualys.com/support/s/article/0000003197>

Certification Paths		
Mozilla Apple Android Java Windows		
Path #1: Trusted		
1	Sent by server	www.tp1rc.edu.tw Fingerprint SHA256: 2b2ed945ed01f5fcae7984ca27dc38316a213d410638fe07ebc3ae4586baac31 Pin SHA256: LnigAYzGXTCIkrlwZ9QsKqfbrlF22C7ucf8hZAzrXNU= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	R3 Fingerprint SHA256: 67add1166b020ae61b8f5c96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TKHSumWb+Fs0Ggogr621gT3PvPKG0= RSA 2048 bits (e 65537) / SHA256withRSA
3	Sent by server In trust store	ISRG Root X1 Self-signed Fingerprint SHA256: 96bce06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6 Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA

多餘根憑證

Extra Root Certificate

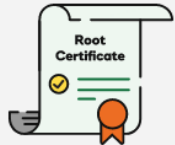
Test Site: www.tp1rc.edu.tw

* <https://ssltools.godaddy.com/views/certChecker>

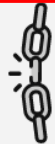
✔ Certificate chain contains extraneous certificate/s, consider using the one provided.

Old Chain

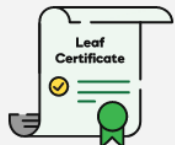
多了根憑證



Serial Number: 8210CFB0D240E3594463E0BB63828B00
Signature Algorithm: Sha256 With RSA Encryption
Issuer Name: Internet Security Research Group
Common Name: ISRG Root X1
Validity Period: June 4, 2015 to June 4, 2035



Serial Number: 912B084ACF0C18A753F6D62E25A75F5A
Signature Algorithm: Sha256 With RSA Encryption
Issuer Name: Internet Security Research Group
Common Name: R3
Validity Period: September 4, 2020 to September 16, 2025

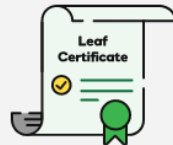


Serial Number: 0334D3018614A322E0A4BB61A4ABDCC3BCA3
Signature Algorithm: Sha256 With RSA Encryption
Issuer Name: Let's Encrypt
Common Name: www.tp1rc.edu.tw
Sans: www.tp1rc.edu.tw
Validity Period: January 6, 2022 to October 8, 2021

New Chain



Serial Number: 912B084ACF0C18A753F6D62E25A75F5A
Signature Algorithm: Sha256 With RSA Encryption
Issuer Name: Internet Security Research Group
Common Name: R3
Validity Period: September 4, 2020 to September 16, 2025



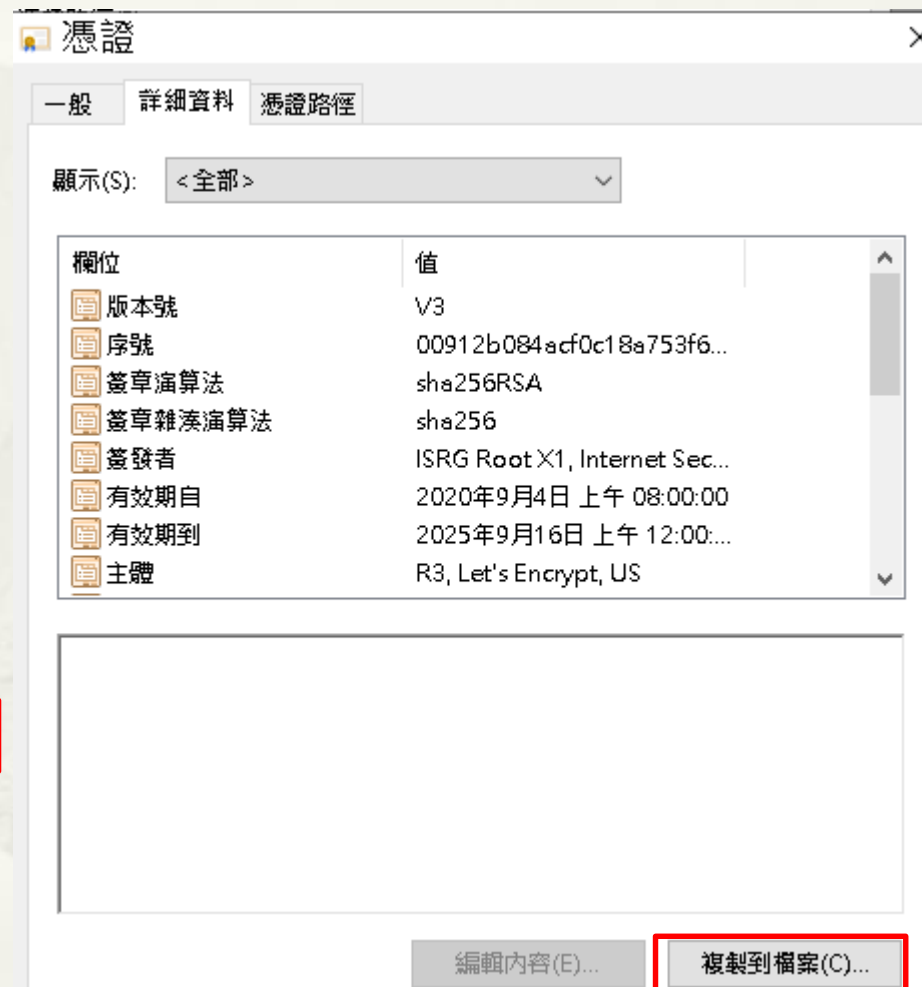
Serial Number: 0334D3018614A322E0A4BB61A4ABDCC3BCA3
Signature Algorithm: Sha256 With RSA Encryption
Issuer Name: Let's Encrypt
Common Name: www.tp1rc.edu.tw
Sans: www.tp1rc.edu.tw
Validity Period: January 6, 2022 to October 8, 2021

How to Fix Certificate Chain Problems

Generate Intermediate Certificate

- * Browser
 - * Chrome
 - * Firefox
- * Online Websites
 - * <https://www.ssllabs.com/ssltest/analyze.html>
 - * <https://whatsmychaincert.com/>
 - * Certificate (PEM format)
 - * Online use hostname
 - * <https://tools.keycdn.com/certificate-chain>
 - * Certificate (PEM format)
 - * <https://certificatechain.io/>
 - * Certificate (PEM format)

Generate Intermediate Certificate Chrome



Generate Intermediate Certificate Chrome

匯出檔案格式

憑證可以用多種檔案格式匯出。

請選取您想要使用的格式：

- ☐ DER 編碼二位元 X.509 (.CER)(D)
- ☒ Base-64 編碼 X.509 (.CER)(S)
- ☐ 密碼編譯訊息語法標準 - PKCS #7 憑證 (.P7B)(C)
 - ☐ 如果可能的話，包含憑證路徑中的所有憑證(I)
- ☐ 個人資訊交換 - PKCS #12 (.PFX)(P)
 - ☐ 如果可能的話，包含憑證路徑中的所有憑證(U)
 - ☐ 如果匯出成功即刪除私密金鑰(K)
 - ☐ 匯出所有延伸內容(A)
 - ☐ 啟用憑證隱私權(E)
- ☐ Microsoft 序列憑證存放區 (.SST)(T)

下一步(N)

取消

要匯出的檔案

請指定您要匯出的檔案名稱

檔案名稱(F):

D:\R3.cer

瀏覽(R)...

完成憑證匯出精靈

您已經成功地完成憑證匯出精靈。

您已指定下列設定：

檔案名稱	D:\R3.cer
匯出金鑰	否
包含憑證路徑中的所有憑證	否
檔案格式	Base64 編碼 X.509 (*.cer)

完成(F)

取消

Generate Intermediate Certificate Firefox

https://www.tp1rc.edu.tw

www.tp1rc.edu.tw 的網站資訊

安全連線

https://www.tp1rc.edu.tw

< www.tp1rc.edu.tw 的連線安全性

您正安全地連線至此網站。

驗證機構: Let's Encrypt

更多資訊

頁面資訊 — https://www.tp1rc.edu.tw/

一般 (G) 媒體 (M) 權限 (P) 安全 (S)

網站身份

網站: www.tp1rc.edu.tw

擁有者: 這個網站沒有提供擁有者資訊。

驗證機構: Let's Encrypt

到期於: 2022年1月6日

檢視憑證

憑證

www.tp1rc.edu.tw R3 ISRG Root X1

主體名稱

一般名稱 www.tp1rc.edu.tw

簽發者名稱

國家 US

組織 Let's Encrypt

一般名稱 R3

其他

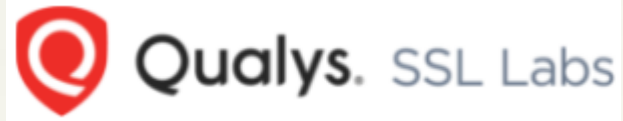
序號 03:34:D3:01:86:14:A3:22:E0:A4:BB:61:A4:AB:DC:C3:BC:A3

簽章演算法 SHA-256 with RSA Encryption

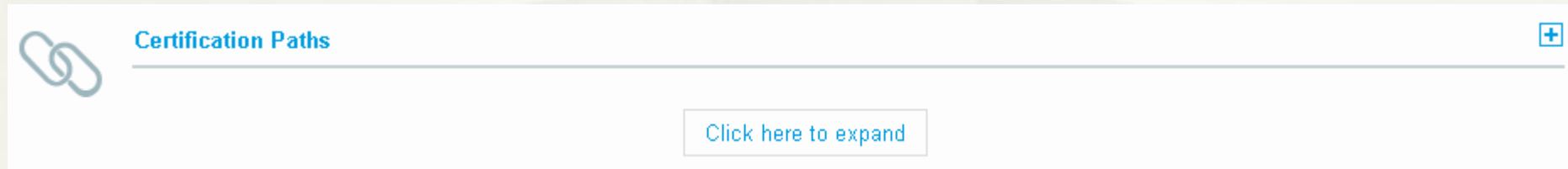
版本 3

下載 PEM (憑證) PEM (金鑰鏈)

Generate Intermediate Certificate Online



* <https://www.ssllabs.com/ssltest/analyze.html?d=www.tp1rc.edu.tw>



Certification Paths


Mozilla Apple Android Java Windows

Path #1: Trusted

1	Sent by server	www.tp1rc.edu.tw Fingerprint SHA256: 2b2ed945ed01f5fcae7984ca27dc38316a213d410638fe07ebc3ae4586baac31 Pin SHA256: LnigAYzGXTClkr/wZ9QsKqfbrlF22C7ucf8hZAzrXNU= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0= RSA 2048 bits (e 65537) / SHA256withRSA
3	Sent by server In trust store	ISRG Root X1 Self-signed Fingerprint SHA256: 96bce06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6 Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA



下載



簡報完畢
謝謝