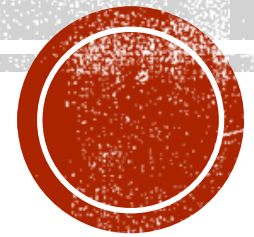


# 免費 SSL 憑證簡介

宜蘭大學區域網路中心



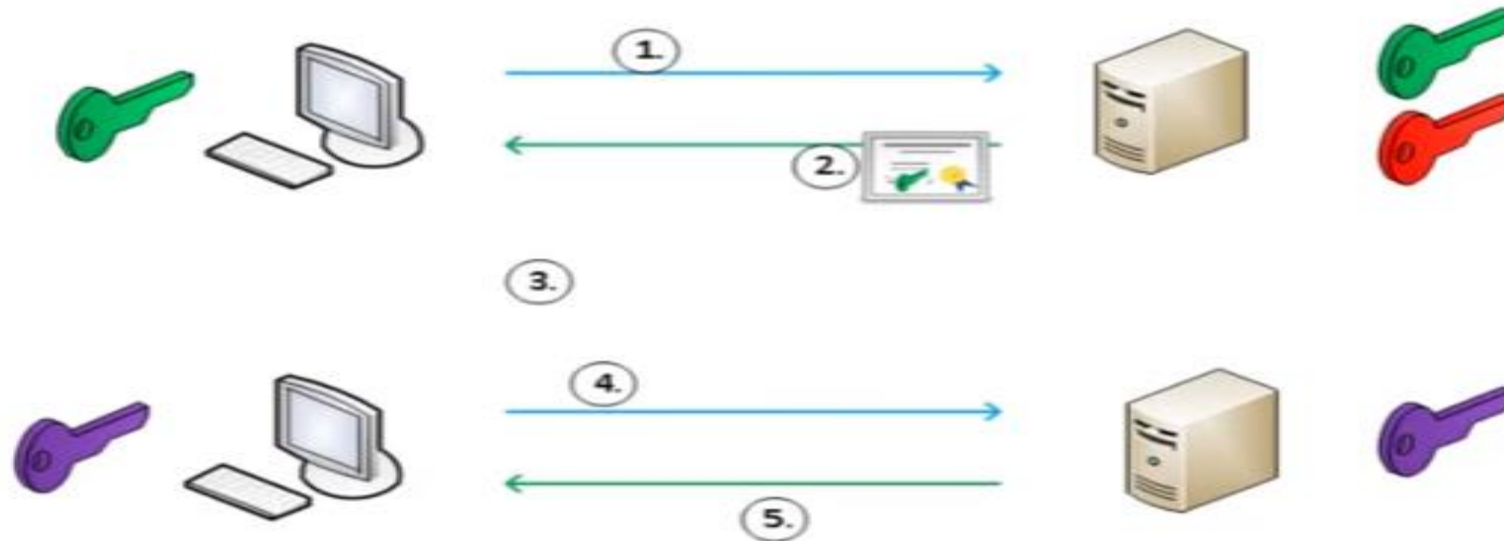
2016.05.18

# WHAT IS SSL/TLS ?

- **SSL (Secure Socket Layer) 安全通訊協定**
  - 一種安全協定，目的是為網際網路通訊，提供安全及資料完整性保障
- **TLS(Transport Layer Security) 傳輸層安全協議**
  - 基於SSL所建立更新、更安全的資料傳輸方式
- **HTTPS、FTPS、SMTPS**
  - HTTP over (SSL/TLS) = HTTPS
  - FTP over (SSL/TLS) = FTPS
  - SMTP over (SSL/TLS) = SMTPS



# SSL/TLS運作方式



[From Youtube : SSL TLS HTTPS process explained in 7 minutes](#)

1. 使用者要求建立SSL連線
2. 網站回應SSL 憑證
3. 使用者透過CA(憑證中心)確認該憑證是正確的
4. 使用者回覆已確認憑證無誤，可以建立連線
5. 網站與使用者間已建立SSL連線



# WHY SSL/TLS ?

Sniffing http Password With Ettercap

# 優缺點

	免費 SSL/TLS 憑證服務	付費 SSL/TLS 憑證服務
優點	簡單化 自動化 快速核發 免費	使用時間長(1~3年) 可人工驗證申請人真實性 安全性較高
缺點	使用期限較短 只能驗證網站所權 無法確認身份 憑證可能被濫用	申請程序繁瑣 核發工作天長 付費

# 一般憑證申請流程

## TWCA SSL伺服器憑證

### 【申請憑證】

對象：新申請TWCA SSL伺服器數位憑證



請將申請憑證所需檢附資料傳真(02)23700728辦理，並請將正本郵寄至本公司留存。

- 『憑證申請單』：請押蓋公司大小章
- 『網站安全認證資料新增異動申請單』：請押蓋公司大小章
- 營利事業登記證影本：請押蓋公司大小章
- TWCA 網域名稱使用授權書：網域名稱非申請單位擁有時請檢附此文件。
- 補充說明：請貴公司（機構）業經詳細審閱「SSL伺服器數位憑證用戶申請註冊及使用須知」及「憑證實務作業基準」之內容，並同意遵守一切規定。本公司（認證中心）保留拒絕簽發憑證之權利，且得免向申請人說明理由；申請經拒絕者，本公司將無息退還已收取之服務費用予申請人。

# 免費SSL憑證服務

- Letsencrypt (ISRG)  
<https://letsencrypt.org/>
- StartSSL(StartCom)  
<https://www.startssl.com/>
- CloudFlare  
<https://www.cloudflare.com/ssl/>
- Wosign(沃通)  
<http://freessl.wosign.com/freessl>
- AffirmTrust  
<http://www.affirmtrust.com/>

# 什麼是LET'S ENCRYPT



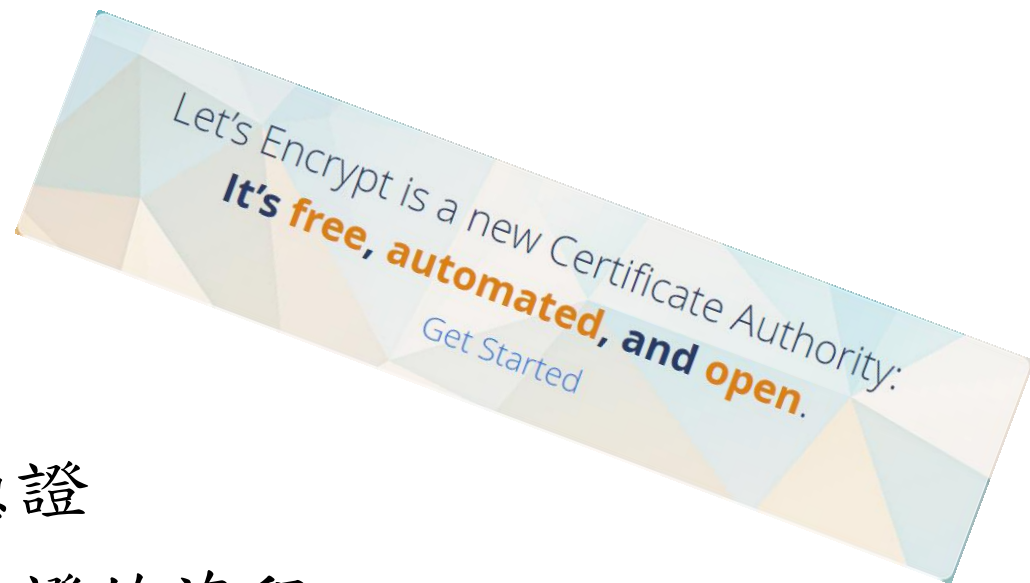
- ISRG於2015年提供的免費憑證簽發服務
- 是一個由多個組織和公司共同資助(Cisco, Akami, Mozilla)
- 提高網際網路安全的非營利性公益組織

基於ACME協議提供了一套**自動化的**證書管理服務  
包括憑證的發行、更新、撤銷等功能  
一切都是**免費的**

2016/4/16 已發行超過170萬個憑證，有380萬個網站使用

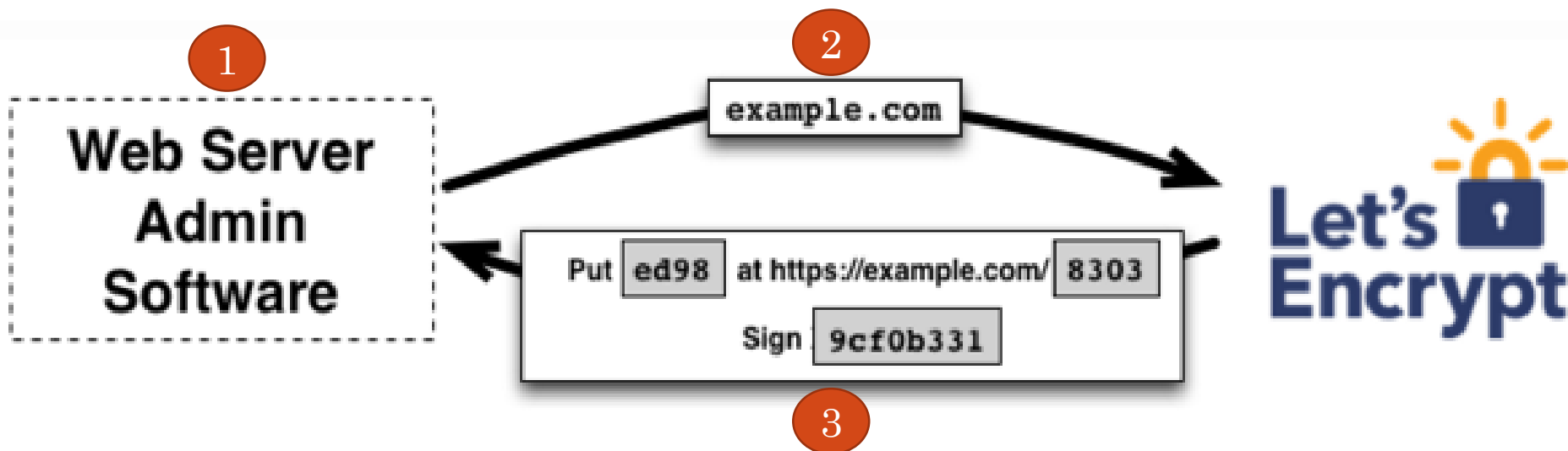


# LET'S ENCRYPT 特色



- **免費**：每個網站都可申請一個免費憑證
- **自動**：在網站主機上可自動化申請憑證的流程
- **安全**：在使用者及憑證機構端，已支援 TLS 的運作
- **透明**：所有憑證的發行與撤銷記錄均可開放給需要調查的人員
- **開放**：提供標準化的API，伺服器可自動申請發行及重新取得憑證
- **互助**：透過社群網站的方式相互交流，解決相關問題

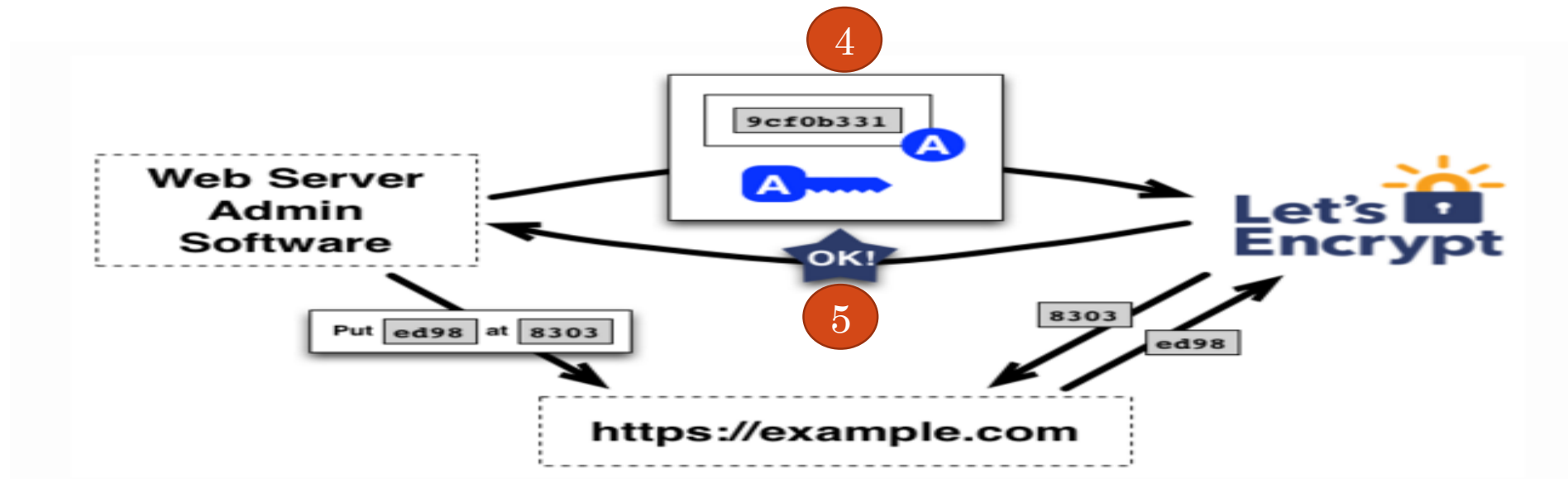
# LET'S ENCRYPT憑證申請流程



1. 在網站伺服器上產生金鑰
2. 通知Let's Encrypt伺服器，要註冊一個網域名稱
3. Let's Encrypt伺服器要求放一個特定的內容在網站上，並可讓外部存取
  - "ed98" = Let's Encrypt提供的序號(9cf0b331)+網站金鑰所產生



# LET'S ENCRYPT 憑證申請流程



4. 網站通知Let's Encrypt已將內容放在網站上
5. Let's Encrypt 確認內容無誤後，發行憑證給網站



# 申請注意事項

- Names/Certificate
  - 一張憑證內，最多可使用100個網域名稱
  - `certbot certonly --webroot -w /var/www/example -d example.com`
- Certificates/Domain
  - 每個domain每個星期最多可以產生20個憑證
    - [blog.example.com]
- Certificates/FQDNset
  - 每個星期每個FQDN組合不可超過5個憑證
    - [www.example.com, example.com]
- Registrations/IP address
  - 在3小時內，單一IP可註冊的次數不可超過500次

# LET'S ENCRYPT 安裝 ~ WINDOWS 篇 (1/8)

- 安裝環境 Windows 2008 R2 + IIS 7.5

1. 下載最新版letsencrypt-win-simple v1.9.0用戶端軟體：

<https://github.com/Lone-Coder/letsencrypt-win-simple/releases/>

2. 然後在目錄中執行letsencrypt命令，進行第一次初始設定

以系統管理員身分執行 letsencrypt.exe

```
C:\Users\██████\Desktop\letsencrypt-win-simple.v1.9.0>letsencrypt.exe
Let's Encrypt (Simple Windows ACME Client)
Renewal Period: 60
Certificate Store: WebHosting

ACME Server: https://acme-v01.api.letsencrypt.org/
Config Folder: C:\Users\██████\AppData\Roaming\letsencrypt-win-simple\httpsacme-v01.api.letsencrypt.org
Certificate Folder: C:\Users\██████\AppData\Roaming\letsencrypt-win-simple\httpsacme-v01.api.letsencrypt.org

Getting AcmeServerDirectory
Enter an email address (not public, used for renewal fail notices):
```



# LET'S ENCRYPT 安裝 ~ WINDOWS 篇 (2/8)

3. 設定你的mail (用於更新失敗通知)

4. 同意 [LE-SA-v1.0.1-July-27-2015.pdf](#) 使用條款

```
Let's Encrypt (Simple Windows ACME Client)
Renewal Period: 60
Certificate Store: WebHosting

ACME Server: https://acme-v01.api.letsencrypt.org/
Config Folder: C:\Users\... \AppData\Roaming\letsencrypt-win-simple\httpsacme-v0
1.api.letsencrypt.org
Certificate Folder: C:\Users\... \AppData\Roaming\letsencrypt-win-simple\httpsac
me-v01.api.letsencrypt.org

Getting AcmeServerDirectory
Enter an email address (not public, used for renewal fail notices): e-mail
...

Calling Register
Do you agree to https://letsencrypt.org/documents/LE-SA-v1.0.1-July-27-2015.pdf?
(Y/N) Y
```



# LET'S ENCRYPT 安裝~WINDOWS 篇 (3/8)

## 5. 選擇您要申請的網站

如下圖所示，選擇1→IIS earth.niu.edu.tw

```
Scanning IIS Site Bindings for Hosts
```

```
1: IIS earth.niu.edu.tw (C:\www)
```

```
W: Generate a certificate via WebDav and install it manually.
```

```
F: Generate a certificate via FTP/FTPS and install it manually.
```

```
M: Generate a certificate manually.
```

```
A: Get certificates for all hosts
```

```
Q: Quit
```

```
Which host do you want to get a certificate for: 1
```



# LET'S ENCRYPT 安裝 ~ WINDOWS 篇 (4/8)

6. 這裡詢問是否需要指定使用者，選擇N

```
Adding Certificate to Store
Closing Certificate Store
Adding https Binding
Committing binding changes to IIS
Opened Certificate Store "My"
Closing Certificate Store
Creating Task letsencrypt-win-simple httpsacme-v01.api.letsencrypt.org with Win
dows Task Scheduler at 9am every day.
Do you want to specify the user the task will run as? <Y/N> N
```

7. 看到此畫面就表示憑證已經自動放入IIS裡面了

```
Do you want to specify the user the task will run as? <Y/N>
Removing existing scheduled renewal IIS earth.niu.edu.tw <C:\www> Renew After 2
016/7/16
Renewal Scheduled IIS earth.niu.edu.tw <C:\www> Renew After 2016/7/16
Press enter to continue.
```





# LET'S ENCRYPT 安裝~WINDOWS 篇 (5/8)

## 8. 檢視 IIS 裡 Let's Encrypt 核發的憑證，有效期限為 90 天

檔案(F) 檢視(V) 說明(H)

連線

起始網頁  
WIN-1MEG010FUEQ (WIN-1M...  
應用程式集區  
站台  
Earth  
earth.niu.edu.tw

伺服器憑證

此功能可用來要求及管理網頁伺服器可與針對 SSL 設定的網站搭配使用的憑證。

名稱	發行給	發行者
earth.niu.edu.tw 2016/5/17 10:37:25 上午	earth.niu.edu.tw	Let's Encrypt Authority X3
earth.niu.edu.tw 2016/5/17 11:15:5 上午	earth.niu.edu.tw	Let's Encrypt Authority X3
earth.niu.edu.tw 2016/5/17 2:35:38 下午	earth.niu.edu.tw	Let's Encrypt Authority X3

憑證

憑證資訊

這個憑證的使用目的如下:

- 確保遠端電腦的識別
- 2.23.140.1.2.1
- 1.3.6.1.4.1.44947.1.1.1

\*請參照憑證授權單位敘述中的詳細資訊。

發給: earth.niu.edu.tw

簽發者: Let's Encrypt Authority X3

有效期自 2016/ 5/ 17 到 2016/ 8/ 15

這個憑證有一個對應的私密金鑰。

簽發者聲明(S)

深入了解憑證

確定

憑證

一般 | 詳細資料 | 憑證路徑

憑證資訊

這個憑證的使用目的如下:

- 確保遠端電腦的識別
- 2.23.140.1.2.1
- 1.3.6.1.4.1.44947.1.1.1

\*請參照憑證授權單位敘述中的詳細資訊。

發給: earth.niu.edu.tw

簽發者: Let's Encrypt Authority X3

有效期自 2016/ 5/ 17 到 2016/ 8/ 15

這個憑證有一個對應的私密金鑰。

簽發者聲明(S)

深入了解憑證

確定

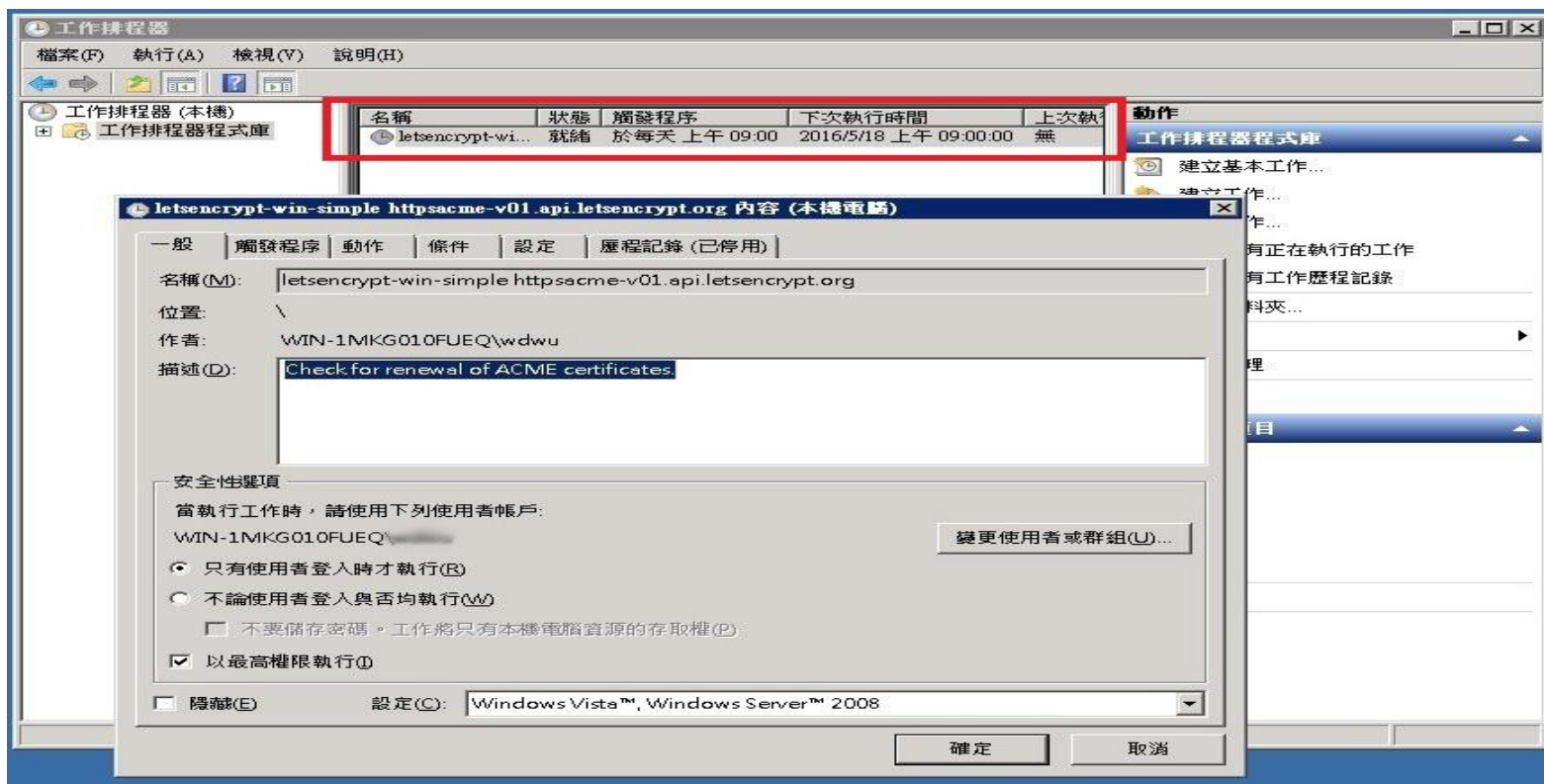


# LET'S ENCRYPT 安裝~WINDOWS 篇 (6/8)

9.檢視工作排程：已自動新增憑證更新的工作排程

排程名稱為：letsencrypt-win-simple httpsacme-v01.api.letsencrypt.org

每天上午09:00檢查並更新，不需擔心憑證90天到期!



# LET'S ENCRYPT 安裝 ~ WINDOWS 篇 (7/8)

10. 擊點瀏覽器左上方網址列綠色鎖頭

檢查網站的憑證有效，並且經過可信賴的第三方單位驗證



# LET'S ENCRYPT 安裝 ~ WINDOWS 篇 (8/8)

Let's Encrypt For Windows Server 申請憑證參考資料

- Official Documentation

<https://letsencrypt.readthedocs.org/en/latest/intro.html>

- Let's Encrypt unofficial Windows Client

<https://github.com/Lone-Coder/letsencrypt-win-simple>

- Let's Encrypt unofficial Windows Client releases

<https://github.com/Lone-Coder/letsencrypt-win-simple/releases/>



# LET'S ENCRYPT 安裝~LINUX篇(1/4)

- 參考網站：<https://letsencrypt.tw/>
- 設定方式 (CentOS + Apache)
  - 安裝必要套件
    - `curl openssl mod_ssl git`
  - 下載letsencrypt.sh
    - `cd ~; git clone https://github.com/lukas2511/letsencrypt.sh.git`
  - 將程式放在指定目錄
    - `mkdir /etc/letsencrypt.sh`
    - `cp ~/letsencrypt.sh/letsencrypt.sh /etc/letsencrypt.sh/`

# LET'S ENCRYPT 安裝~LINUX篇 (2/4)

- 設定方式 (CentOS)
  - 設定 config.sh 並建立對應目錄
    - `echo "WELLKNOWN=/var/www/letsencrypt" > /etc/letsencrypt.sh/config.sh`
    - `mkdir -p /var/www/letsencrypt`
  - 在 Apache 設定檔中新增路徑
    - `Alias /.well-known/acme-challenge/ /var/www/letsencrypt/` (Let's Encrypt 會到該目錄中確認驗證內容)
  - 產生 SSL certificate
    - `/etc/letsencrypt.sh/letsencrypt.sh -c -d <要申請的網域名稱>`

```
+ Responding to challenge for letsencrypt.tw...
+ Challenge is valid!
+ Requesting certificate...
+ Checking certificate...
+ Done!
+ Creating fullchain.pem...
+ Done!
```

# LET'S ENCRYPT 安裝 ~ LINUX 篇 (3/4)

- 設定方式 (CentOS)
  - 確認是否有成功產生憑證
    - `ls /etc/letsencrypt.sh/certs/<網域名稱>/` (會有 cert、chain、fullchain、privkey 等檔案)
  - 修改 Apache 的 SSL 設定 (`/etc/httpd/conf.d/ssl.conf`)
    - `SSLCertificateFile /etc/letsencrypt.sh/certs/<網域名稱>/cert.pem`
    - `SSLCertificateChainFile /etc/letsencrypt.sh/certs/<網域名稱>/chain.pem`
    - `SSLCertificateKeyFile /etc/letsencrypt.sh/certs/<網域名稱>/privkey.pem`
  - 重新啟動 Apache
    - `service httpd restart`



# LET'S ENCRYPT 安裝~LINUX篇(4/4)

- 自動檢查並更新憑證
  - 編輯 `/etc/cron.d/letsencrypt-letsencrypt_tw`
  - 新增下列內容
    - `0 0 * * * root sleep $(expr $(printf "\%d" "0x$(hostname | md5sum | cut -c 1-8)") \%`  
`86400); ( /etc/letsencrypt.sh/letsencrypt.sh -c -d <網域名稱>; /usr/sbin/service apache2`  
`reload ) > /tmp/letsencrypt.sh-/<網域名稱>.log 2>&1`





# DigiCert® SSL Installation Diagnostics Tool

letsencrypt.niu.edu.tw

Check for common vulnerabilities

CHECK SERVER

✓ DNS resolves letsencrypt.niu.edu.tw to 120.101.0.22

HTTP Server Header: Apache

✓ SSL certificate

Common Name = letsencrypt.niu.edu.tw  
Subject Alternative Names = letsencrypt.niu.edu.tw  
Issuer = Let's Encrypt Authority X3  
Serial Number = 033CA36E0C977E21862C29BC36AA85CE12A3  
SHA1 Thumbprint = 03DD4381624CA3F32E4079C64940227C5C6755E4  
Key Length = 4096  
Signature algorithm = SHA256 + RSA (excellent)  
Secure Renegotiation: Supported

✓ SSL Certificate has not been revoked

OCSP Staple: Not Enabled  
OCSP Origin: Good  
CRL Status: Not Enabled

✓ SSL Certificate expiration

