如何使用 MakeCert 建立開發測試用途的自簽憑證 (Self-Signed Certificate)

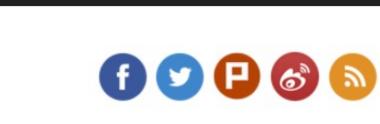
認識 PKI 架構下的數位憑證格式與憑證格式轉

换的心得分享 →



← 如何使用 PowerShell 建立開發測試用途的自

簽憑證 (Self-Signed Certificate)



隱藏側邊欄 (Ctrl+B) 登入





搜尋... 搜尋 每月文章

■ 團隊合作 (9) ■ 網路管理 (18)

專業證照

Microsoft^{*}

CERTIFIED

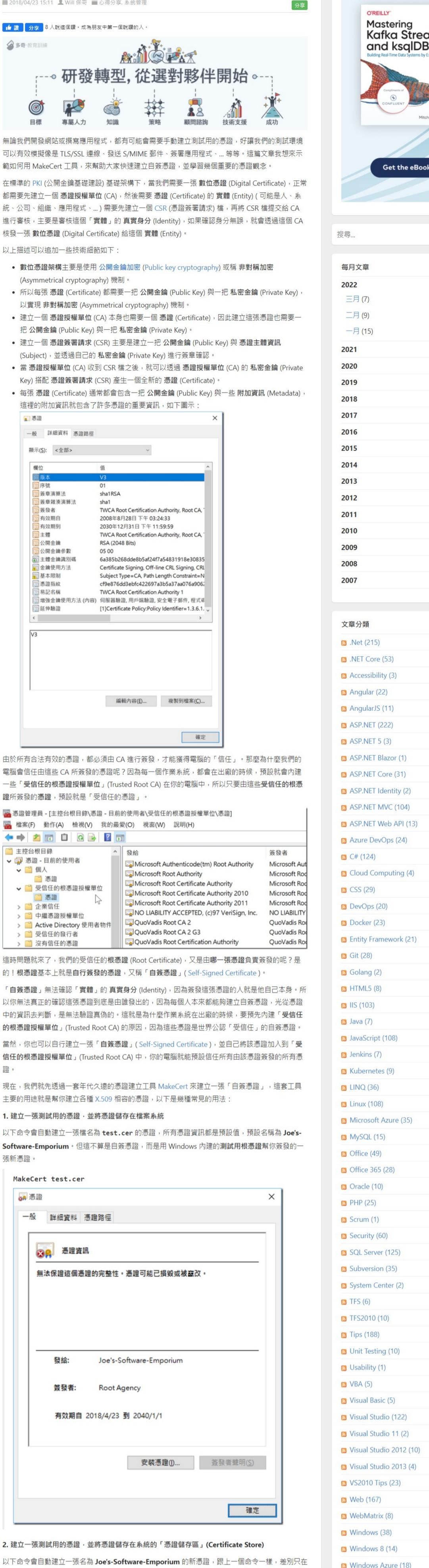
Professional Developer

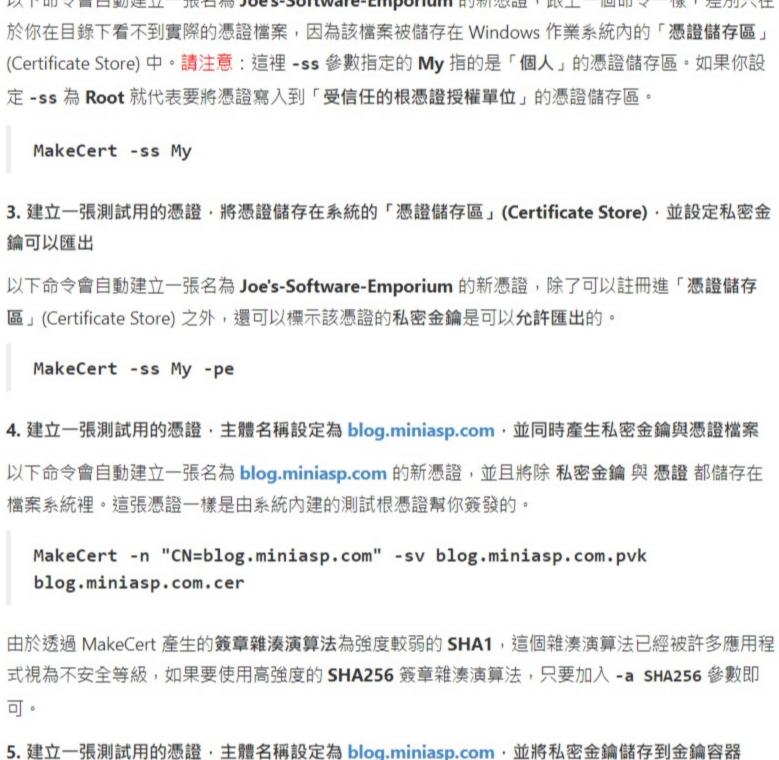
Microsoft^{*} CERTIFIED

> Technology Specialist

Web Developer 4

.NET Framework 4, Web Applications





MakeCert -n "CN=blog.miniasp.com" -sk MyKey blog.miniasp.com.cer 6. 建立一張測試用的「自簽憑證」·主體名稱設定為 blog.miniasp.com·並同時產生私密金鑰與 憑證檔案 以下命令會自動建立一張名為 blog.miniasp.com 的新憑證,並且將除 私密金鑰 與 憑證 都儲存在 檔案系統裡。由於我們加上了 - r 參數,所以你將會產生一份「自簽憑證」,所以你可以看到「簽發

MakeCert -n "CN=blog.miniasp.com" -sv blog.miniasp.com.pvk

這裡的-sk 參數是設定一個 金鑰容器 的名稱,並將 私密金鑰 儲存到該 金鑰容器 中,用這種方式

儲存私密金鑰會比儲存到檔案系統相對來的安全許多!因為儲存在金鑰容器中的私密金鑰只能透過

CryptoAPI 來取得相關資訊,微軟並沒有提供任何命令列工具幫你單獨匯出私密金鑰。不過也有人

寫了個 KeyPal 工具 (Source Code) 幫你管理 金鑰容器。想了解更深入,可以參考 Key Storage and

(Key Container)·將憑證儲存到檔案系統

者」的名稱將會跟「主體名稱」一樣,如下圖示:

詳細資料 憑證路徑

blog.miniasp.com.cer -r

發給:

簽發者:

Retrieval 文件。

∞ 憑證

憑證資訊 這個 CA 根憑證不受信任。如果您要啟用信任,請將這個憑證安裝到 信任根憑證授權單位存放區。

安裝憑證(1)...

簽發者聲明(S)

blog.miniasp.com

blog.miniasp.com

有效期自 2018/4/23 到 2040/1/1

X



強型密鑰用法), 並指定正確的 OID (物件識別碼)。在建立憑證時常見的 OID 如下:

如果我們想建立一張可以給 IIS 網站伺服器專用的自簽憑證,就可以用以下命令快速建立:

MakeCert -n "CN=blog.miniasp.com" -ss My -r -pe -sr localmachine -

請注意:你必須將憑證註冊在 LocalMachine 才能讓 IIS 選到這個憑證。如果你沒有指定 -eku 參

• 1.3.6.1.5.5.7.3.1 - 伺服器驗證 (serverAuth)

• 1.3.6.1.5.5.7.3.2 - 用戶端驗證 (clientAuth)

• 1.3.6.1.5.5.7.3.3 - 程式碼簽署 (codeSigning)

• 1.3.6.1.5.5.7.3.8 - 時戳簽章 (timeStamping)

eku 1.3.6.1.5.5.7.3.1

⋒ 憑證

欄位

相關文章

2022 香魚馬

Scott Hanselman

Git 實戰 - 將檔案從歷史 Commit 中移除

主機的本機帳號登入錯誤

【茶包射手筆記】AD Domain Controller 出現某

Using Home Assistant to integrate a Unifi Pro...

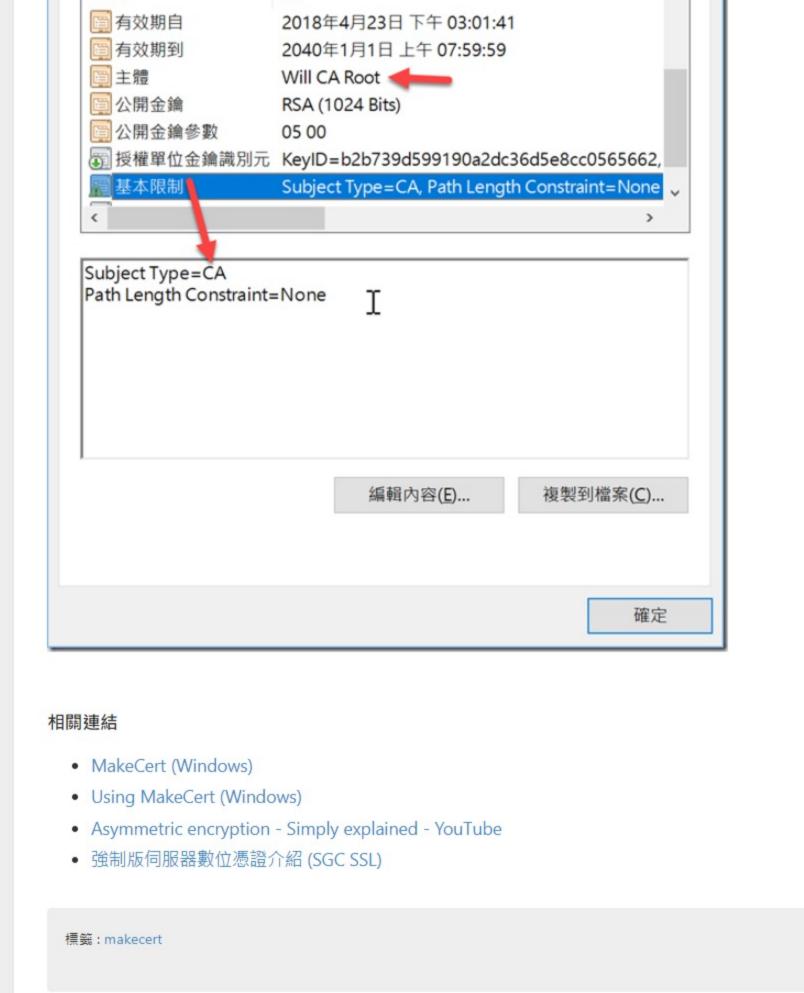
一般 詳細資料 憑證路徑

顯示(S): <全部>

• 1.3.6.1.5.5.7.3.4 - 電子郵件加密 (emailProtection)

數,也可以從 IIS 選中這張憑證,因為沒有設定參數就是一張萬用的憑證。但如果你將 -eku 設定為 1.3.6.1.5.5.7.3.2 (clientAuth) 的話,IIS 在選取憑證的時候,就不會看見這張憑證。 除了憑證可以指定用途以外,其實還能設定「憑證類型」(Certificate Type),大致區分兩類: 1. end (終端實體) 。 這種類型的憑證,主要用在實際的系統或應用程式中。 2. authority (憑證授權單位) 。 這種類型的憑證,主要用在 CA 憑證授權單位中,用來簽發其他 end 憑證之用。 請注意:如果你沒有特別設定,該憑證一樣也是萬用憑證,兩種類型都可以用。 如果你想建立一張 CA 的自簽憑證,可以用以下方式建立: MakeCert -n "CN=Will CA Root" -ss Root -r -pe -sr localmachine -cy authority 如下圖示:

X





如何使用 MakeCert 建立開發測試用途的自簽憑證 (Self-Signed Certificate)

如何使用 PowerShell 建立開發測試用途的自簽憑證 (Self-Signed Certificate)

無論我們開發網站或撰寫應用程式,都有可能會需要手動建立測試用的憑證,好讓我們的測試環境可以有效模擬像是 TLS/SSL 連線...

前篇文章我們學會了用老牌的 MakeCert 建立自簽憑證 (self-signed certificates),對於大部分數位憑證的需求已經綽綽有餘,確實...



本網站對於任何使用或引用本網站網頁資料