

中華電信通用憑證管理中心 (PublicCA)

計算主體金鑰識別元/碼

聲明：本說明文件之智慧財產權為中華電信股份有限公司（以下簡稱本公司）所有，本公司保留所有權利。本說明文件所敘述的程序係將本公司安裝相關軟體的經驗分享供申請 SSL 伺服器軟體憑證用戶參考，若因參考本說明文件所敘述的程序而引起的任何損害，本公司不負任何損害賠償責任。

目錄

Windows 系統產製之金鑰.....	2
OpenSSL 工具產製之金鑰.....	4
Keytool 工具產製之金鑰.....	5

Windows 系統產製之金鑰

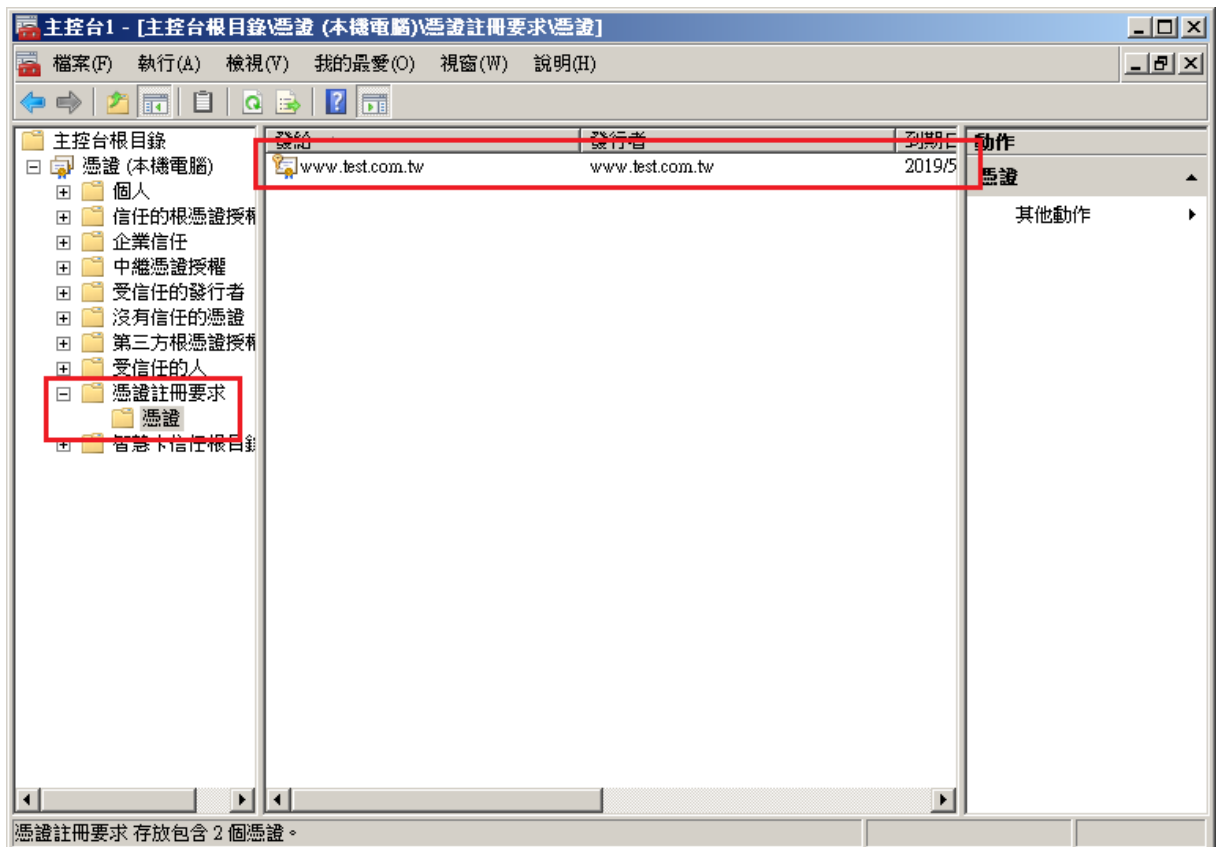
以下操作僅適用於 Server 2008(R2)、2012(R2)、2016 版本。

1. 開啟 MMC 主控台。

- 「新增/移除嵌入式管理單元」
- 「憑證」→「新增」
- 「電腦帳戶」→「下一步」→「完成」
- 「確定」

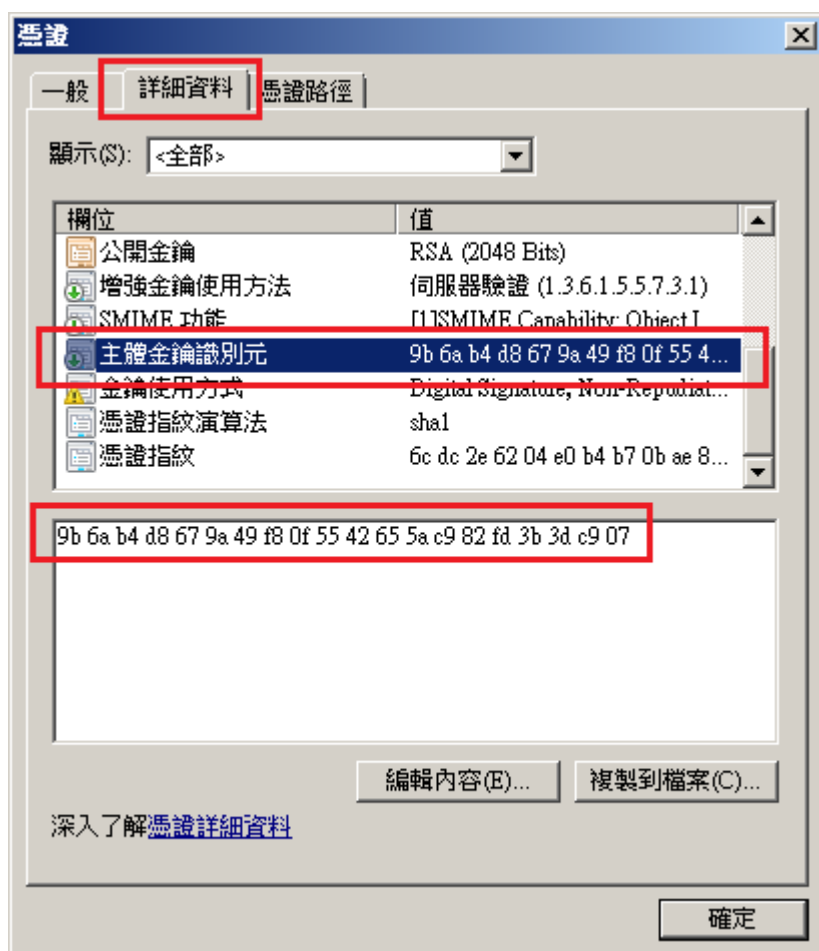
找到左邊的「憑證註冊要求」→「憑證」

當您產製完憑證請求檔後，憑證註冊要求預設會出現一筆資料，若您有多筆，可依照到期日找到最新的一筆資料，並點開憑證。



2. 點選「詳細資料」→「主體金鑰識別元/碼」

範例數值為：9b 6a b4 d8 67 9a 49 f8 0f 55 42 65 5a c9 82 fd 3b 3d c9 07

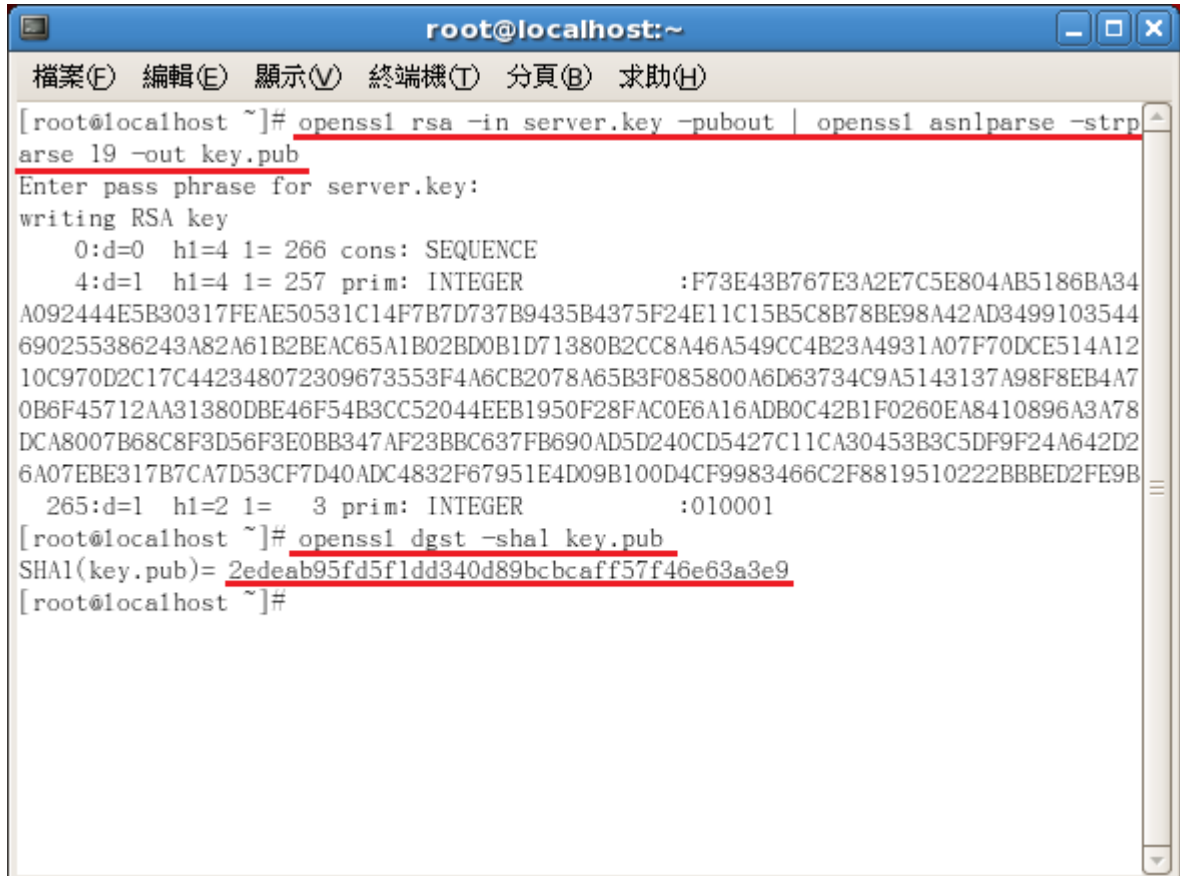


OpenSSL 工具產製之金鑰

1. 輸入指令：

```
$ openssl rsa -in <server.key 檔案位置> -pubout | openssl asn1parse -strparse 19 -out <key.pub 儲存路徑>
```

```
$ openssl dgst -sha1 <key.pub 檔案路徑>
```



```
root@localhost:~  
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)  
[root@localhost ~]# openssl rsa -in server.key -pubout | openssl asn1parse -strparse 19 -out key.pub  
Enter pass phrase for server.key:  
writing RSA key  
  0:d=0  hl=4  l= 266 cons: SEQUENCE  
  4:d=1  hl=4  l= 257 prim: INTEGER           :F73E43B767E3A2E7C5E804AB5186BA34  
A092444E5B30317FEAE50531C14F7B7D737B9435B4375F24E11C15B5C8B78BE98A42AD3499103544  
690255386243A82A61B2BEAC65A1B02BD0B1D71380B2CC8A46A549CC4B23A4931A07F70DCE514A12  
10C970D2C17C442348072309673553F4A6CB2078A65B3F085800A6D63734C9A5143137A98F8EB4A7  
0B6F45712AA31380DBE46F54B3CC52044EEB1950F28FAC0E6A16ADB0C42B1F0260EA8410896A3A78  
DCA8007B68C8F3D56F3E0BB347AF23BBC637FB690AD5D240CD5427C11CA30453B3C5DF9F24A642D2  
6A07EBE317B7CA7D53CF7D40ADC4832F67951E4D09B100D4CF9983466C2F8819510222BBBED2FE9B  
 265:d=1  hl=2  l=   3 prim: INTEGER           :010001  
[root@localhost ~]# openssl dgst -sha1 key.pub  
SHA1(key.pub)= 2edeab95fd5f1dd340d89bcbcaff57f46e63a3e9  
[root@localhost ~]#
```

2. 最後計算結果即為主體金鑰識別元/碼。

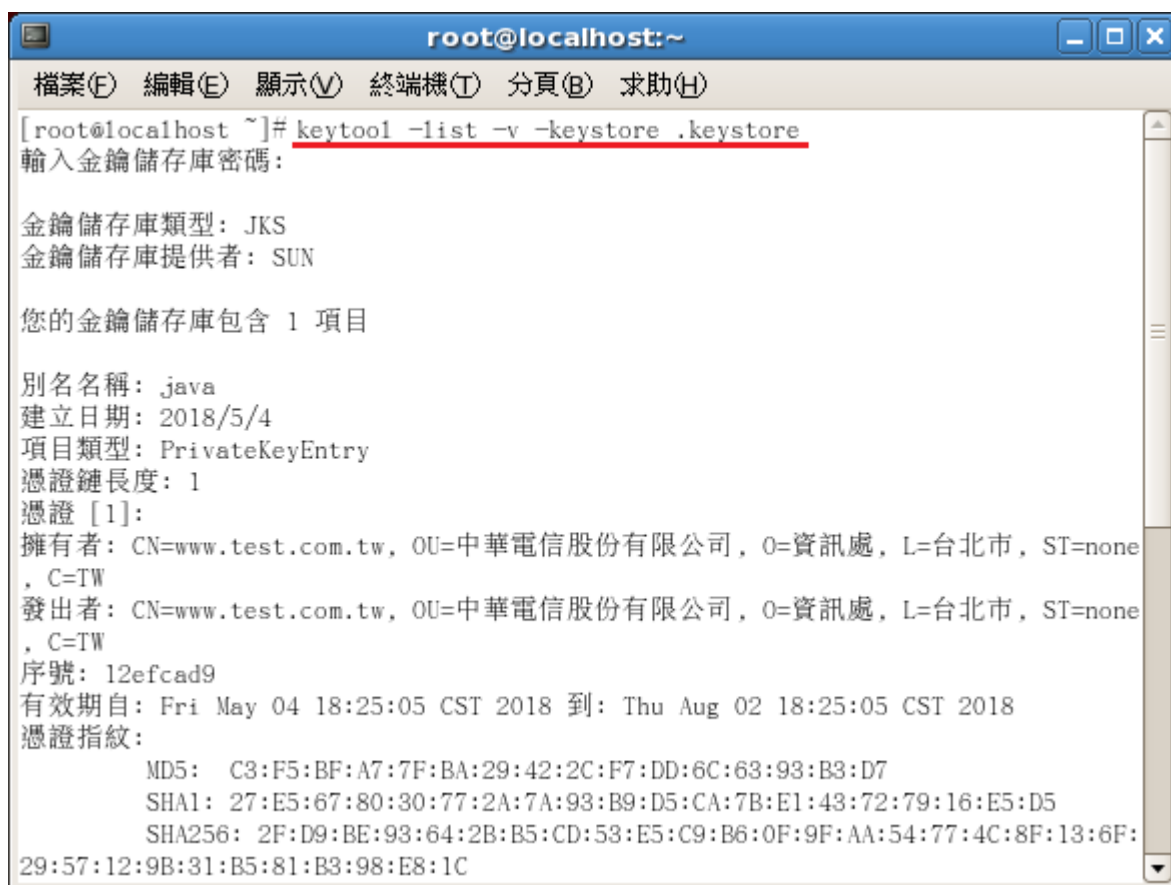
範例數值為：2e de ab 95 fd 5f 1d d3 40 d8 9b cb ca ff 57 f4 6e 63 a3 e9

Keytool 工具產製之金鑰

以下操作僅適用於 Java 7 之後版本產生之 keystore 檔案。

1. 輸入指令

```
$ keytool -list -v -keystore <.keystore 檔案路徑>
```



```
root@localhost:~  
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)  
[root@localhost ~]# keytool -list -v -keystore .keystore  
輸入金鑰儲存庫密碼:  
  
金鑰儲存庫類型: JKS  
金鑰儲存庫提供者: SUN  
  
您的金鑰儲存庫包含 1 項目  
  
別名名稱: java  
建立日期: 2018/5/4  
項目類型: PrivateKeyEntry  
憑證鏈長度: 1  
憑證 [1]:  
擁有者: CN=www.test.com.tw, OU=中華電信股份有限公司, O=資訊處, L=台北市, ST=none, C=TW  
發出者: CN=www.test.com.tw, OU=中華電信股份有限公司, O=資訊處, L=台北市, ST=none, C=TW  
序號: 12efcad9  
有效期自: Fri May 04 18:25:05 CST 2018 到: Thu Aug 02 18:25:05 CST 2018  
憑證指紋:  
    MD5:  C3:F5:BF:A7:7F:BA:29:42:2C:F7:DD:6C:63:93:B3:D7  
    SHA1: 27:E5:67:80:30:77:2A:7A:93:B9:D5:CA:7B:E1:43:72:79:16:E5:D5  
    SHA256: 2F:D9:BE:93:64:2B:B5:CD:53:E5:C9:B6:0F:9F:AA:54:77:4C:8F:13:6F:  
29:57:12:9B:31:B5:81:B3:98:E8:1C
```

2. 確認項目類型為「PrivateKeyEntry」

並確認 SubjectKeyIdentifier 下，紅線數值

範例數值為：00 09 35 22 b2 8c 2b 8c 23 cd b2 e3 f0 69 8d 6c b8 c5 09 7b

```
root@localhost:~
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
MD5: C3:F5:BF:A7:7F:BA:29:42:2C:F7:DD:6C:63:93:B3:D7
SHA1: 27:E5:67:80:30:77:2A:7A:93:B9:D5:CA:7B:E1:43:72:79:16:E5:D5
SHA256: 2F:D9:BE:93:64:2B:B5:CD:53:E5:C9:B6:0F:9F:AA:54:77:4C:8F:13:6F:
29:57:12:9B:31:B5:81:B3:98:E8:1C
簽章演算法名稱: SHA256withRSA
版本: 3

擴充套件:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 00 09 35 22 B2 8C 2B 8C 23 CD B2 E3 F0 69 8D 6C ..5" ..+.#....i.1
0010: B8 C5 09 7B .....
]
]

*****
*****

[root@localhost ~]#
```