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。

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。

🧱 主接台1 - [主接台根目錄\憑證 (本機電腦)	틆證註冊要求\틆證]		<u>- 🗆 ×</u>
🔚 檔案(F) 執行(A) 檢視(V) 我的最愛(O)	視窗(₩) 說明(H)		_ 8 ×
🗢 🔿 🙍 🗊 📋 🧟 😹 🚺 📅			
☐ 主控台根目錄		到期日勤作	
🖃 🗊 憑證 (本機電腦) 🛛 🖾 www.test.com.tv	www.test.com.tw	2019/5	_
 □ □ □ □ ○ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □		其他動作	•
■ □ 企業信仕			
 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □			
🕀 🛄 沒有信任的憑證			
Ⅲ □ 第三方根憑證授和			
□ 憑證			
🗉 💼 智慧卡倍性根目			
·····································		J	

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

造設	×
一般詳細資料	
顯示(S): <全部>	
欄位	值
	RSA (2048 Bits)
る で か 留 短 金 踊 使 用 万 法 一 一 一 の に の 一 の 法 一 一 の し の の の し つ し の つ し つ し の し の し の し の し の し の し の し の し の し つ こ つ つ つ し つ つ し つ つ し つ し つ し つ し つ し つ し つ し つ つ つ し つ つ つ つ し つ つ つ つ つ つ つ つ つ つ つ つ つ	何服器競證 (1.3.5.1.5.5.7.3.1) [1]SMIME Canability: Object I
1000 主體金鑰識別元	9b 6a b4 d8 67 9a 49 f8 0f 55 4
■ <mark>■ 金綸使用方式</mark> ■ 憑證指紋演算法	Digital Signature, Non-Repudiat
	6c dc 2e 62 04 e0 b4 b7 0b ae 8 💌
9b 6a b4 d8 67 9a 49 f8 0f 55 42 65	5 5a c9 82 fd 3b 3d c9 07
ž	編輯內容(E) 複製到檔案(C)
深入了解憑證詳細資料	
	確定

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	@localh	ost:~		
檔案(E) 編輯(E)	顯示(⊻)	終端機①	分頁(B)	求助(出)		
[root@localhost	~]# opens	ss1 rsa -i	n server	.key -pubout	openss1 asnl	parse -strp
arse 19 -out key	/.pub					
Enter pass phras	se for sei	rver.key:				
writing RSA key	1 000	CEOUE	NOD			
0:d=0 h1=4	1= 266 cc	ons: SEQUE	NCE	- PEOP (OP		44051000404
4:d=1 h1=4	1= 257 pi	14E7D7D70	EK ZDO 40ED 4	:F73E43B	TOTESAZETUSE80	4AB5180BA34
A092444E3B303171	EAESUSSI AG1D9DEAC4	35 A 1 DAODDA	7 6943364 01071990	010F24E11010B	2000/000900420 240224/0214070	270DCE514412
100020002408024	1016266400 2480723006	373553F446	CR207846	583E08580046D	C4D23A4931A07F 62724C94514219	70DCE514A12
0B6F45712AA3138	DRF46F54F	336652044F	EB1950F2	SEACOF6A16ADB	0C42B1F0260FA8	410896A3A78
DCA8007B68C8F3D3	56F3E0BB34	47 AF23BBC6	37FB690A	D5D240CD5427C	11CA30453B3C5D	F9F24A642D2
6A07EBE317B7CA7I)53CF7D40/	ADC4832F67	951E4D09	B100D4CF99834	66C2F881951022	2BBBED2FE9B
265:d=1 h1=2	1= 3 ри	im: INTEG	ER	:010001		
[root@localhost	~]# opens	ss1 dgst -	shal key	.pub		
SHA1(key.pub)=	2edeab95f	15f1dd340d	89bcbcaf	f57f46e63a3e9		
[root@localhost	~]#					
						*

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:~ 🗕 🗖	X)
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)	
[root@localhost ~]# <u>keytool -list -v -keystore .keystore</u> 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=IW 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	•

 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(E) 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:E1:43:72:79:10 SHA256: 2F:D9:BE:93:64:2B:B5:CD:53:E5:C9:B6:0F:9F:AA:54:77 29:57:12:9B:31:B5:81:B3:98:E8:1C 簽章演算法名稱: SHA256withRSA 版本: 3	6:E5:D5 :4C:8F:13:6F:		
擴充套件:			
<pre>#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 6C5"+.#. 0010: B8 C5 09 7B]]</pre>	i.1		
[root@localhost ~]#	- -		