# GPG (The GNU Privacy Guard) 操作說明

# 一、鑰匙對製作

# (一)執行 GPG 製作鑰匙對

1.點選程式集之 GPGshell 下選擇 GPGkeys。



## 2.點選【金鑰】下拉選單,點選【新增】。

🔒 GPGke	ys							- 🗆 🛛
檔案 (E)	金鑰(仏) 群組(仏) 信任(工) 特	撿視(Y)	執	(行 (1) 偏好設定 (1	E) 說明(H)			
SN ++ -	新增 (N)	Ctrl+N		📕 🖉 B+ 🚦	? 🔤 🗸	<find i<="" th=""><th>n List&gt;</th><th></th></find>	n List>	
▲ 使用者	匯出 (全部)(x)			大小 主信 證	信 打造	逾期	描述	
	匯入 (2)							
	從金鑰伺服器上更新 (全部)(a)		F					
	瀏覽金鑰伺服器 (Y)	Ctrl+K						
	匯出 (E)	Ctrl+E						
	刪除 (D)	Ctrl+D						
	撤銷 (R)							
	編輯 (1)		F					
	指紋 (E)	Ctrl+F1						
	于鑰	Ctrl+F2						
	使用者 ID	Ctrl+F3			1			
	PGP 封包 (P)	Ctrl+F4		3月11日版辞(広) 52				
🤜 DSA: 0	资草 (11)	Ctrl+F5			0.0 K	(B) 0.0 KB	0.0 KB 2009/9/16 上午	= 11:35 🦷
	加入群組		F					
	複製到剪貼簿		ŀ					
	從金續伺服器更新		Ľ					
	运主金曜何服器							
	寄信 (M)	Ctrl+M	_					

3.出現如下畫面,「姓名」欄輸入【key???】(???為單位代碼,本範例為key979);「電子郵件」欄輸入報名單位在大考中心登錄之聯絡信箱;「有效期限」設定鑰匙對的有效期限(本範例為2010年8月31日),亦可不設定期限(鑰匙對永遠有效)。完成後按【打造】鍵。

🔒 GPGkeys	- Key Genera	tion					
金鑰:		-子鑰:					
類型: RS.	A	類型:	RSA				
大小: 204	8 💌	大小:	2048	-			
_使用者 ID:							
姓名:	key979						
備註:							
電子郵件:	test@tp.edu.tw						
-> key979 <te< th=""><td>st@tp.edu.tw&gt;</td><th></th><td></td><td></td></te<>	st@tp.edu.tw>						
有效期限:							
年份: 2010 ▼ 月份: 08 ▼ 日: 31 ▼							
🏼 進階選項	預設 (		打造取消	Ø			

4.出現如下畫面開始製作鑰匙對,完成後會自動關閉。



# 5.出現如下畫面,按【是】鍵。

GPGke	ys 🛛 🛛 🕅
?	Your new key 0x9FB27DDC is not protected by a passphrase yet! Do you want to change this now?
	The passphrase needs to be entered twice. When done, type QUIT and save the changes with Y.
	To add/change the passphrase later, choose the "Passphrase" item from the "Key(s)/Edit" menu.
	<u> </u>

6.自行設定「密碼(密語)」,至少6個字元,輸入後按【Enter】鍵。
☎ c:/windows/system32/cmd.exe
gpg (GnuPG) 1.4.10; Copyright (C) 2009 Free Software Foundation, Inc. This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law.
gps: 正在檢查信任資料庫
gps: 3 個勉強信任以及 1 個完全信任是 PGP 信任模型的最小需求
gps: 深度: 0 有效: 1 已簽署: 0 信任: 0-, 0q, 0n, 0m, 0f, 1u
gps: 下次信任資料庫檢查將於 2010-08-30 進行
私鑰可用.
pub 2048R/9FB27DDC 建立: 2009-09-16 到期: 2010-08-30 用途: SCA 信任: 徹底 有效性: 徹底
sub 2048R/091D0E05 建立: 2009-09-16 到期: 2010-08-30 用途: E
[ 徹底 ] (1). key983 <test@tp.edu.tw>
這把金鑰未被保護.
請輸入要給這把私鑰用的新密語.
請輸入密語:

## 7. 再次輸入「密碼(密語)」後按【Enter】鍵。

🔤 c:\windows\system32\cmd.exe
gpg (GnuPG) 1.4.10; Copyright (C) 2009 Free Software Foundation, Inc. This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law.
sps: 正在檢查信任資料庫 sps: 3 個勉強信任以及 1 個完全信任是 PGP 信任模型的最小需求 sps: 深度: 0 有效:  1 已簽署:  0 信任: 0-, 0q, 0n, 0m, 0f, 1u sps: 下次信任資料庫檢查將於 2010-08-30 進行 私鑰可用.
pub 2048R/9FB27DDC 建立: 2009-09-16 到期: 2010-08-30 用途: SCA 信任: 徹底
L 徹底 」(1). key983 <test@tp.edu.tw> 這把金鑰未被保護. 請輸入要給這把私鑰用的新密語.</test@tp.edu.tw>
請再輸入一次密語:

🗴 大學入學考試中心 College Entrance Examination Center 🔌

8.先出現「指令>」輸入「quit」後,按【Enter】鍵。接著出現「要儲存變更嗎?」輸入

# 「y」後,按【Enter】鍵。

sx c:/windows/system32/cmd.exe gpg (GnuPG) 1.4.10; Copyright (C) 2009 Free Software Foundation, Inc. This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law. gps: 正在檢查信任資料庫 gps: 3 個勉強信任以及 1 個完全信任是 PGP 信任模型的最小需求 gps: 深度: 0 有效: 1 已簽署: 0 信任: 0-, 0q, On, Om, Of, 1u gps: 下次信任資料庫檢查將於 2010-08-30 進行 私鑰可用. pub 2048R/9FB27DDC 建立: 2009-09-16 到期: 2010-08-30 用途: SCA 信任: 徹底 有效性: 徹底 sub 2048R/091D0E05 建立: 2009-09-16 到期: 2010-08-30 用途: E [ 徹底 ] (1). key983 <test@tp.edu.tw> 這把金鑰未被保護. 請輸入要給這把私鑰用的新密語.

9.出現如下畫面,表示鑰匙對已產生。

🗟 GPGkeys						
檔案 (E) 金鑰 (K) 群組 (L	) 信任(I) 檢視	(12) 執行(11)	偏好設定	(P) 説明(	H)	
\$¶. ++• e=> e=> ==> 💀	4 2 1 1	n 🤹 🐂 🟉	<u>//</u>   8+	: ? 📼	✓ <find< p=""></find<>	in List>
▲ 使用者 ID	金鑰 ID 大小	主信 證信	打造	逾期	描述	
≪9key979 <test@tp.edu.tw></test@tp.edu.tw>	0x150C2232 2048	Ultim. Ultim.	2009/9/16	2010/8/30	RSA key pai	r (last added) 👌
重新載入金鑰 OX			аж (K)	=>		
🤜 DSA: 0 📢 ELG: 0 📢 RSA: 1	已選取: 0/1 把金鑰		1.2 KB 2	.5 KB 2.0 KB	2009/9/16	下午 02:35

## (二)匯出公鑰及私鑰

1. 選取欲匯出之鑰匙對(如本範例 key979),點選【金鑰】下拉選單,點選【匯出】。

🚨 GP	Gk	eys				
檔案(	Ð	金鑰 (K)	群組 (L)	信任 (I)	檢視 (V)	執行 (m) 偏好設定 (P) 説明 (H)
5¶. (*	⊛ ∢	新增 ①	D		Ctrl+N	🗊 🙅 💩 💈 🎖 🔤 ▾ 🛛 <find in="" list=""></find>
▲ 使月 ≪9key	用者 /979	匯出 (3 匯入 (p 從金鑰 瀏覽金	È部)(x) ) 伺服器上頭 鑰伺服器 (	更新 (全部)(a 卫)	) Ctrl+K	證信 打造 逾期 描述 Jltim. 2009/9/16 2010/8/30 RSA key pair (last added) ▶
		び回答 (E)	D D D		Ctrl+E Ctrl+D	
		編輯(1	)			•
		指紋 (E 子鑰 使用者 PGP 封 簽章 (u	) ID 包 (2) )		Ctrl+F1 Ctrl+F2 Ctrl+F3 Ctrl+F4 Ctrl+F5	L 2 3 4 5
		加入群	組 剪貼簿			> >
j	重新:	് 從金鑰 送至金	伺服器更新 鑰伺服器	ҥ		▶ 論伺服器 ( <u>K</u> ) □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
🛁 DSA	4: O	寄信 (1	<u>۵</u>		Ctrl+M	1.2 KB 2.5 KB 2.0 KB 2009/9/16 下午 03:01

2.選擇儲存公鑰檔的目錄(資料夾)(如本範例之公鑰檔【key979.asc】儲存於[大考報名] 資料夾中),將原預設之檔名 key979 (0x150C2232) pub.asc 改為 key???.asc (???為單 位代碼,如本範例 key979),再按【儲存】鍵。

另存新檔					2 🛛
儲存於①:	▶ 大考報名		•	← 🗈 💣 📰▼	
桌面					
分析					
JAH JAH					
我的電腦					
網路上的芳鄰					
	檔名(N):	key979.asc		•	儲存(S)
	存檔類型(I):	Key files (*.asc)	$\mathcal{I}$	•	取消

3.按【確定】鍵,即完成匯出公鑰,請將該檔案於報名期間內傳送至本中心。

GPGke	ys 🛛 🛛
(į)	Selected public key exported to file: "C:大考報名\key979.asc"
	User ID: key979 <test@tp.edu.tw> Key ID: 0xFB36D3F9150C2232</test@tp.edu.tw>
	確定

4.出現如下之畫面後,請按【是(Y)】匯出私鑰。

GPGkeys 🛛
Export secret key?
是(Y) 否(N)

5.出現如下畫面,選擇匯出目錄(資料夾)後按【儲存】鍵。

另存新檔							2 🛽
儲存於(l):	▶ 大考報名			-	+ 🗈 💣		
ま 我最近的文件 で 東面 予 我的文件 で 教的文件 で 教的文件 で 和 本 和 路上的芳本 本 本 本 本 本 の 本 の 、 、 、 、 、 、 、 、 、 、 、 、 、	Aey979.asc						
	檔名(N):	key979 (0x1500	C2232) sec.asc			•	儲存(S)
	存檔類型(I):	Key files (*.asc	)			•	取消
重新載入金鑰	0x	*	金鑰伺服器(丛)	l ⊂>	· .		
		/1 把全输	12	KB 25	KB 20KB	2009/9/16	下午 03:08

6.按【確定】鍵,即完成匯出私鑰。



7. 匯出之公鑰、私鑰檔名如下圖,請將該檔案備份並儲存安全之處備用。

😂 C:\大考報名		×
: 檔案(E) 編輯(E) 檢	視(V) 我的最愛(A) 工具(I) 說明(H) 🥂 🦧	
🕒 上一頁 🔹 🕥 🗸	- 🏂 🔎 搜尋 💫 資料夾 🕼 🍞 🗙 🌱 💷 🔹	»
資料夾 × 名稱 🔺	大 類型 修改日期	T
	<u>0x150C2232) sec.asc</u> 4 KB PGP Armored File 2009/9/16 下午 03:09 sc2 KB PGP Armored File 2009/9/16 下午 03:10	i I
	公鑰 私鑰	

※請妥善保存備份的公鑰檔及私鑰檔,若原有的鑰匙對不慎遺失或更換電腦, 可將備份檔案匯入使用。

## 二、資料簽章

須簽章之資料為報名資料檔:學科能力測驗為 AO???.txt、術科考試為 DO???.txt、指 定科目考試為 BO???.txt (???為單位代碼)。使用本中心集體報名作業軟體者,執行轉 出後,檔案存在<u>指定目錄</u>下《如學測及術科為 C:\\*\*Sat\data、指考為 C:\\*\*Drse\data (\*\* 為學年度)》。

#### 1.點選程式集之 GPGshell 下選擇 GPGtools。



2.螢幕出現如下畫面,點選第3個項目。



3.點選要簽章的文件(如本範例 AO979.txt),選擇【開啟】。

Sign (detached)					2 🔀
查詢(I):	🗀 data		•	← 🗈 💣 📰 ▼	
我最近的文件	A0979.txt				
<b></b> 夏面					
武的文件					
我的電腦					
1 網路上的芳鄰					
	檔名(N):	A0979.txt		•	開啓(Q)
	檔案類型(I):	All files (*.*)		•	取消

### 第7頁.共13頁

4.選擇簽章鑰匙 key??? (如本範例 key979),按【OK】鍵。

B GPGtools - Sign (detached)				
		☐ ASCII封裝 🔮		
◆ 以此金鑰簽署	金鑰 ID	大小		
🖦 key979 <test@tp.edu.tw></test@tp.edu.tw>	0x150C2232	2048		
		<u>0</u> K	取消 ( <u>C</u> )	

5.輸入「密碼(密語)」(產生鑰匙對時設定的密碼)後,按【Enter】鍵。

🗠 c:\windows\system32\cmd.exe	_ 🗆 🗙
妳需要用密語來解開下列使用者的 私鑰: ˝key979 <test@tp.edu.tw>˝ 2048 位元長的 RSA 金鑰, ID 150C2232, 建立於 2009-09-16</test@tp.edu.tw>	
請輸入密語: ■	
注音 半:	► ► //.

6.完成後,指定目錄中會產生簽章檔 AO???.txt.sig(如本範例 AO979.txt.sig)。



## 三、資料驗證

本中心傳送各項試務資料檔案(如准考證清冊及試場分配表檔案)及成績檔時,均使用電 子簽章,各報名單位須使用本中心「考試專用公鑰」(以 ceec??.asc 命名,??為西元年度,例 ceec2011.asc)來核驗並確認檔案。使用報名作業軟體完成安裝 GPG 者,已內含本中心「考 试專用公鑰」,或請洽本中心第二處取得本中心公鑰,並將其匯入貴單位之簽章軟體內。 (一) 匯入大考中心考試專用公鑰 (下列說明以 ceeckey.asc 為例)

1.點選程式集之 GPGshell 選擇 GPGkeys。

🖻 GPGkeys 檔案 (E) 金鑰 (K) 群組 (L) 信任 (I) 檢視 (V) 執行 (u) 偏好設定 (P) 說明 (H) SIL 4-3 4 新增 (N)... Ctrl+N 🗊 🙅 🕬 💈 😤 📼 🗸 <Find in ▲ 使用者 大小 主信 證信 打造 逾期 匯出(全部)(x)... 🦚 key979 201078 Ulf 1 IIt 200979 匯入(2). 從金鑰伺服器上更新 (全部)(a) • 瀏覽金鑰伺服器 (V)... Ctrl+K 匯出 (E)... Ctrl+E 刪除 (D)... Ctrl+D 撤銷 (R)... ۲ 編輯① 指紋 (E) Ctrl+F1 子鑰 Ctrl+F2 使用者 ID Ctrl+F3 PGP 封包 (P) Ctrl+F4 簽章 (11) Ctrl+F5 加入群組 ۲ 複製到剪貼簿 < > 從金鑰伺服器更新 送至金鑰伺服器 ٠ 3鑰伺服器(K) ⇔ 重新: 寄信 (M) Ctrl+M KB 2.5 KB 2.0 KB 2009/9/16 下午 03:55 \varTheta DSA: 0

2.點選【金鑰】下拉選單,點選【匯入】。

3.出現選取檔案視窗,選取 ceecKey.asc, 按【開啟】。

開啓					2 🔀
查詢(I):	🗅 大考報名		•	← 🗈 💣 📰▼	
我最近的文件 していた 泉面 我的文件 我的文件 我的電腦	Ceeckey.asc				
網路上的芳鄰					
	檔名(N): 檔案類型(T):	ceeckey.asc Key files (*.asc; *.gpg; *.pgp; *.pl	kr; *.sk	r) 💌	開啓(Q) 取消

#### 第9頁.共13頁

🗴 大學入學考試中心 College Entrance Examination Center 🔌

🖻 GPGkeys 檔案 (E) 金鑰 (K) 群組 (L) 信任 (T) 檢視 (Y) 執行 (n) 偏好設定 (P) 説明 (H) 왜 🕶 📾 🕬 🔤 🗛 🔟 🖌 🖉 🖄 🐂 🖓 📾 🗸 🔿 💈 🕋 🔻 <Find in List> ▲ 使用者 ID 金鑰ID | 大小 | 主信 | 證信 | 打造 逾期 描述 🤜 ceeckey <examdp@ceec.edu.tw> 0x776E23A7 10... 2009/9/.. Never DSA public key (l --📾 key979 <test@tp.edu.tw> 0x150C2232 20... Ultim. Ultim. 2009/9/... 2010/8/30 RSA key pair < > 0x 金鑰伺服器(丛) ⇒ | 重新載入金鑰 ன DSA:1 📢 ELG:0 ன RSA:1 已選取:0/2 把金鑰 2.3 KB 2.5 KB 2.0 KB 2009/9/16 下午 04:03

4.出現如下畫面即表示成功匯入大考中心「考試專用公鑰」(如本範例 ceecKey)。

5.出現下列視窗,按【關閉】。

^
=
×
>
ЯĦ( <u>C</u> )

## (二)檢查資料檔是否被更改

本範例中的資料檔為【SatL\_979.xls】,簽章檔為【SatL\_979.xls.sig】。

1.點選程式集之 GPGshell 下選擇 GPGtools。

2.螢幕出現如下畫面,點選最後一個項目(Deprypt/Verify)。



3.點選簽章檔(如本範例 SatL\_979.txt.sig),按【開啟】。

Decrypt/Verify/(I	import)				2 🔀
查詢(I):	▶ 大考報名		•	⇐ 🗈 📸 🕶	
我最近的文件 「」」 東面 我的文件 我的文件 一 我的文件 一 一 和 路上的芳鄰	BatL_979.xls.sig				
	檔名(N):	SatL_979.xls.sig		•	開啓(0)
	檔案類型(I):	GnuPG files (*.asc; *.gpg; *.pgp;	; *.sig)	•	

4.出現圖一字樣表示資料檔 SatL\_979.xls 未被更改過;圖二字樣則表示資料檔被更改過。

圖一:「完好的簽章...」表示資料未被更改過。

B GPGtools - Output of Decrypt/Verify	
gpg: 由 2009/9/16 16:07:46 建立的簽章, 使用 RSA 金鑰 ID 150C2232 gpg: 完好的簽章來自於 "key979 <test@tp.edu.tw>"</test@tp.edu.tw>	^
File: C:\大考報	
完好的簽章<	>
複製到剪貼簿 (b) MDC: ◎ SIG: ●	閉( <u>C</u> )

## 圖二:「損壞的簽章...」表示資料被更改過。

B GPGtools - Output of Decrypt/Verify	- • 🛛
gpg: 由 2009/9/16 16:07:46 建立的簽章,使用 RSA 金鑰 ID 150C2232	~
gpg: *項摄* 的簽草來自於 "key979 <test@tp.edu.tw>"</test@tp.edu.tw>	
File: C:\大考報名\Sata an xls.sig	
Time: 2009/9/16 04:11:57 下午,19/14/16 08:11:57 上午 UTC)	*
<	>
Dennym	
	朔 ( <u>C</u> )

# 第11頁.共13頁

## 四、資料解密方式

本中心傳送之加密成績檔 H???.csv.gpg (???為單位代碼,例如:單位代碼為 979 的加密成績 檔為 H979.csv.gpg),係以各單位報名時之公鑰 key???.asc 加密,開啟檔案時需以各報名單位 之鑰匙對及密碼解密。解密後之成績檔為 H???.csv,解密方式如下:

1.點選程式集之 GPGshell 下選擇 GPGtools。

2.螢幕出現如下畫面,點選最後一個項目(Deprypt/Verify)。



3.點選要解密的檔案(如範例 H979.csv.gpg),點選【開啟】。

Decrypt/Verify/(	Import)			2
查詢(I):	🗀 大考報名	•	← 🗈 💣 📰 マ	
しています。 我最近的文件	≥H979.csv.gpg			
泉面				
我的電腦				
網路上的芳鄰				
		H979.csv.gpg	•	開啓(Q)
	檔案類型(I):	GnuPG files (*.asc; *.gpg; *.pgp; *.sig)	-	取消

4. 輸入「密碼(密語)」(產生鑰匙對時設定的密碼)後,按【Enter】鍵。

🔤 c:\windows\system32\cmd.exe	
妳需要用密語來解開下列使用者的 私鑰: ~ceeckey <exam@tp.edu.tw>~ 2048 位元長的 RSA 金鑰, ID E9E33754, 建立於 2009-09-16 (主要金鑰 ID 172269CA)</exam@tp.edu.tw>	
請輸入密語: _	

5.出現下圖字樣表示解密成功及簽章無誤,按【關閉】鍵。



6.完成後,在相同目錄下會產生 H???.csv(如範例 H979.csv)。

