PGP (Pretty Good Privacy Suite) 操作說明

一、鑰匙對製作

(一)執行 PGP 製作鑰匙對

1.點選 PGPkeys (點選 【Programs】 → 【PGP】 → 【PGPkeys】)。

(※如點選【程式集】→【PGP】→【空】會無法開啟 PGP 請依上列方式操作)

- IVIA	N1977	_	_						
Ē	Programs	▶	Ē	ΡC	βΡ	►	(Documentation	•
	DesignPro						88	PGPkeys	
۰	Windows Update						2	PGPtools	
1	WinZip						٨	PGPtray	
i	捷徑 - 程式集								
S .	啓動 Outlook Express								
🥎 -	設定程式存取及預設値								
a	開啓 Office 文件								
٤.	新增 Office 文件								
	Windows 檔案總管								
()	积式亀(₽)	•							
-	1mm 女性(III)	•							
- 1	大(〒)2) 鉛完(5)								
The second secon	地名(1)								
à	12(手(丘)								
÷.	航沙1(山) 劫/긎(□)								
-	₩/IJ(IZ)								
Ø	關機(∐)								
	第始 🛛 🖄 🗭 🛃 🎩 🖸	8	0	0	9				

2.產生新的鑰匙對(先將系統中原有之預設值鑰匙對或不需用之鑰匙對刪除)。

💦 PGP	keys						_ 🗆 X
<u>E</u> ile <u>E</u> d	it <u>V</u> iew	<u>K</u> eys <u>S</u> erv	er <u>G</u> roups	Help			
🧠 🛪 🖉	ଣ କ୍ଷା ବ୍	Sign					
Keys				Ctrl+D	Trust	Size	Description
		<u>A</u> dd		•			
		Enable					
		Disable					
		Keventy					
		<u>N</u> ew Key	r	Ctrl+N			
		Share Sp	lit				
		I <u>m</u> port		Ctrl+M			
		Export		Ctrl+E			
		Propertie		Ctrl+I			
					-		
							/
							/

3.鑰匙對包含「Public Key」(公鑰)及「Private Key」(私鑰)。選擇【下一步】。

Key Generation Wizard		×
2-2-	In order for other people to send you secure messages, you must generate a key pair.	
LP N	Your key pair will also be used to sign digital documents.	
mar 1	A key pair consists of a "Public Key," and a "Private Key." The public key should be given to everyone you know (PGP has facilities to assist in this). The private key should be kept absolutely secret.	
PGP	If you would like more information on what a key pair is and how PGP works, click the Help button, below.	
	Otherwise, choose Next to continue.	
[<上一步(B) [下一步(D)) 取消 説明	

4.輸入鑰匙對連結的 Full name 及 Email address 之後,選擇【下一步】。Full name 以【key???】命名(???為單位代碼,本範例為 key979)。

Key Generation Wizard		×	
PGP	What name and email address should be associated with this key pair? By listing your name and email address here, you let your correspondents know that the key they are using belongs to you. Eull name: key979 Email address: test@tp.edu.tm		報名單位在大考中 心登錄之聯絡信箱
	_<上一步(B) 下一步(D) > 取消 説明	J	

5.點選【Diffie-Hellman/DSS】,選擇【下一步】。

	What two of key would you like to concrete? If you don't know it's
a to	recommended that you generate a Diffie-Hellman/DSS key pair.
2	RSA is the "old-style" PGP key. Most new users of PGP will be expecting a Diffie-Hellman/DSS key.
	If you'd like more information on the differences between the two key types, press the Help button, below.
PGP	Key Pair Type © Diffie-Hellman/DSS © BSA

6.點選【2048 bits】,選擇【下一步】。

Key Generation Wizard	How large a key pair do you wish to generate? As a rule, larger keys are more secure, but slower. For most applications, 1024 - 2048 bit keys are quite sufficient. Key Pair Size C 1024 bits
PGP	 C 1024 bits C 1536 bits (1536 Diffie-Hellman/1024 DSS) © 2048 bits (2048 Diffie-Hellman/1024 DSS) C 3072 bits (3072 Diffie-Hellman/1024 DSS) C Qustom (1024 - 4096 bits) 2048

7.點選【Key pair never expires】(鑰匙對永遠有效),選擇【下一步】。

ey Generation Wizard	You can set your key pair to automatically expire within a certain amount of time. When your key pair expires, you will no longer be able to use it for encrypting or signing. However, it will still decrypt and verify. Once you generate your key pair, you will not be able to change its expiration setting. Key Expiration Key pair never expires Key pair never expires Key pair gapires on
	< 上一步 (B) 下一步 (D) > 取消 說明

8.自行設定密碼,至少8個字元,其中必須包含一個數字(本範例中密碼設定為 12345678),再次輸入確認密碼後,選【下一步】。(請務必牢記自行設定之密碼)

Key Generation Wizard		×
	Your private key will be protected by a p you do not write this passphrase down. Your passphrase should be at least 8 cl contain non-alphabetic characters. Passphrase:	bassphrase. It is important that haracters long and should
PGP	Passphrase Quality :	× •
	Confirmation:	
	12345678	A V
	<上─毋(B) 下─毋(N) >	取消

9.請依螢幕指示點選【下一步】,直至以下畫面即表示已經產生 PGP Key pair(PGP 鑰匙對),選擇【完成】。

Key Generation Wizard	×
	Congratulations! You have just generated a PGP key pair!
	You will now be able to receive secure messages and sign documents.
	If you wish to send your key to the server at a later date, simply right click on it in PGPkeys, and use the "Send to" menu item.
PGP	Click Finish below to add your new key to your keyring!
	<上一步(B) 完成 取消 說明

(二)匯出 Public Key(公鑰)

1. 選取欲匯出之鑰匙對(如本範例 Key979)。

😽 PGPkeys				- 🗆 🗙					
Eile Edit View Keys Server Groups Help									
ା 🛪 🗳 🎯 ୯. ୧୯ କ୍ର 🗽 🖬									
Keys	Vali Trust	Size	Description						
🖃 🎭 key979 <test@tp.edu.tw></test@tp.edu.tw>	🧑 <u>77777</u>	2048/1024	DH/DSS key pair						
🖻 📧 key979 <test@tp.edu.tw></test@tp.edu.tw>	0		User ID						
🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉			DSS exportable sign	nature					
<u> </u>									
1 key(s) selected				1.					



I P GPkeys					- 🗆 🗙
Eile Edit View 🥱 🗶 🏹 🖓	Keys Server Group Sign Set as Default Key	>s Help Ctrl+S Ctrl+D	Size	Description	
□ % key979 <tes< b=""> □ * key979 <tes □ * key979 <tes □ * key979 <</tes </tes </tes<>	Add Enable Disable Reyoke Reverify Signatures		2048/1024	DH/DSS key pair User ID DSS exportable signature	
	<u>N</u> ew Key Share S <u>p</u> lit	Ctrl+N			
	Import	Ctrl+M			
1 key(s) selected	Export	Ctrl+E			14
	Properties	Ctrl+I			

- 3.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 [My Documents] 資料夾中),點選【存檔】即完成。

J PGPkeys						- 🗆 ×
Eile Edit View Keys Server G	roups H	lelp				
🤏 🗶 🎯 🔍 😤 🃚 🗃						
Keys	Vali	Trust	Size	Description		
⊨ wey979 <test@tp.edu.tw> ⊨ wey979 <test@tp.edu.tw></test@tp.edu.tw></test@tp.edu.tw>	(¥7777	2048/1024	DH/DSS key 1 User ID	pair	220
key979 <test@tp.edu.tw></test@tp.edu.tw>				DSS exportabl	le signature	
Export Key to File						? ×
	cuments				_r	
						-
1 keye						
檔案名稱(N): key979.asc					存檔(S)	
存檔類型(T)· ASCILKey	File (* as	sc)		-	取消	
in month of the second						1
Include Private Key(s)						
Include <u>6</u> .0 Extensions						

(三)備份鑰匙對

1.點選鑰匙對(如本範例 Key979)。

1 PGPkeys					_ 🗆 🗙	
Eile Edit View Keys Server Groups Help						
역 🗶 🔏 🥪 🤍 약 等 🔭 🖨 🖬						
Keys	Vali	Trust	Size	Description		
🖃 🎭 key979 <test@tp.edu.tw></test@tp.edu.tw>	(77777	2048/1024	DH/DSS key pair		
🗄 🚾 key979 <test@tp.edu.tw></test@tp.edu.tw>	0			User ID		
∽🗛 key979 <test@tp.edu.tw></test@tp.edu.tw>				DSS exportable signature		
1 key(s) selected					11.	

第4頁.共10頁

2.點選【Keys】下拉選單,選取【Export】。



3.選擇儲存鑰匙對檔案的目錄(資料夾),將檔案名稱改為 key???bak.asc (如本範例

key979bak.asc),並勾選【Include Private Key(s)】選項如下圖,再點選【存檔】。



4. 關閉視窗(點選×),選擇 【Don't Save】離開軟體。



※請妥善保存備份的鑰匙對 key???bak.asc,若原有的鑰匙對不慎遺失或更換電腦, 可將此備份鑰匙對匯入使用。

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.開啟 PGPtools,點選【Sign】(如下圖箭頭指示)出現選取檔案視窗,再選取要簽章的文件 AO???.txt ,點選【開啟】。
 - (亦可不開啟 PGPtools,先自指定目錄下選取 AO???.txt ,按滑鼠右鍵選取【PGP】→選取 【Sign】,直接進入下個步驟畫面)

Select File(s) to S		2 🗙
搜尋位置(I):	🔄 data	▼ ← € 💣 💷 ▼
A0979.txt		
檔案名稱(N):	AO979.txt	開啓(Q)
檔案類型(I):	All Files (*.*)	▼ 取消 Clipboard

2.輸入密碼(產生鑰匙對時設定的密碼),選擇【OK】。(若軟體中存在多副鑰匙對,必須 自下拉選單中選擇正確的鑰匙對,如本範例 key979)

PGPtools - Enter Passphrase	? ×
Signing key: key979 <test@tp.edu< td=""><td>w> (DSS/1024)</td></test@tp.edu<>	w> (DSS/1024)
Enter passphrase for above key:	
12345678 ✓ Detached Signature ✓ Iext Output	

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



第6頁.共10頁

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。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. 開啟【PGPkeys】, 點選【Keys】下拉選單, 點選【Import】。

PGPkeys				
<u>Eile E</u> dit <u>V</u> iew	<u>Keys</u> Server G	oups <u>H</u> elp	1	
🤧 X 🔏 🌒 Q	<u>S</u> ign			
Keys	Set as Default K	ey Ctrl+D	ty Trust Size D	escription
🗄 🧒 key979 <test< td=""><td>Add</td><td></td><td>2048/1024 D</td><td>H/DSS key pa</td></test<>	Add		2048/1024 D	H/DSS key pa
	Enable			
	Disable			
	Reverify Signatu			
	New Key	Ctrl+N		
	Share Split			_
•		0.1.14		
	Import	Ctrl+M	-	
	Export	Ctrl+E		
		Ctrl+I		

2.出現選取檔案視窗,選取 ceeckey.asc,點選【開啟】。

Select File Conta	ining Key				2 🔀
查詢(I):	🗀 My Documents		•	≠ 🖬 🏜 🖬 ▼	
我最近的文件	Diceeckey.asc)				
「桌面					
) 我的文件					
了。 我的電腦					
1 網路上的芳鄰					
	檔名(N):	ceeckey.asc		•	開啓(Q)
	檔案類型(I):	Text Files (*.txt; *.asc)		•	取消

3.點選【Import】。

8 Select key(s)				2 🛛		
Select the key(s) you would like to import to your keyring :						
Keys	Validity	Trust	Size	Description		
庄 🗁 ceeckey <examdp@ceec.edu.tw></examdp@ceec.edu.tw>	٩		2048/1024	DH/DSS public key		
<						
	11		\frown			
<u>S</u> elect All	Unsele		<u>I</u> mport	<u>C</u> ancel		
				7		
	<u></u>		\checkmark			

第7頁.共10頁

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

4.出現如下圖示即完成匯入大考中心「考試專用公鑰」(ceeckey. asc)。

J ¶ PGPkeys					
Eile <u>E</u> dit <u>V</u> iew <u>K</u> eys <u>S</u> erver <u>G</u>	roups <u>H</u> elp				
🥦 🗙 🔏 📽 🔍 🛫 👻 😂 😂 I					
Keys	Validity	Trust	Size	Description	Key ID
ceeckey <examdp@ceec.edu.tw></examdp@ceec.edu.tw>	-		2048/1024	DH/DSS public key	0x776E
占 📧 ceeckey <examdp@ceec.edu< td=""><td>•)</td><td></td><td></td><td>User ID</td><td></td></examdp@ceec.edu<>	•)			User ID	
🗸 ceeckey <examdp@ceec.ed< td=""><td></td><td></td><td></td><td>DSS exportable signature</td><td>0x776E</td></examdp@ceec.ed<>				DSS exportable signature	0x776E
·					

(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】。 開啟簽章檔【SatL_979.xls.sig】(double click),

出現圖一表示資料檔 SatL_979.xls 未被更改過,圖二表示資料檔被更改過。

圖一 資料檔未被更改過

	🗳 PG Plog			
	Name	Signer	Validity	Signed
(🖉 \$atL_979.xls	ceeckey <examdp@ceec.edu.tw></examdp@ceec.edu.tw>	👷 2008/9/22	下午 02:53:53
	\mathbf{P}			
	<	Ш		>

圖二 若資料檔被更改過,則簽章檔會出現「×」

🗳 PGPlog				
Name	Signer	Validity		Signed
🖍 SatL_979.xls	ceeckey <examdp@ceec.edu.tw></examdp@ceec.edu.tw>		Bad Signature	
\sim				
			_	
<				>

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。解密方式如下:

1.點選【PGPtools】。

Programs	►	👼 PG P	•	-	Documentation	•
\land DesignPro			8	P	PGPkeys	
🧐 Windows Update				9	PGPtools	
🖳 WinZip			é	B	PGPtray	
🗟 捷徑 - 程式集			_			
🗐 啓動 Outlook Express						
😏 設定程式存取及預設値						
🗃 開啓 Office 文件						
🕙 新增 Office 文件						
🔍 Windows 檔案總管						
□ 程式集(P)	►					
	►					
№ 設定(S)	►					
3 搜尋(C)	►					
参 說明(H)						
킾 執行(R)						
● 閣機(1)						
🏽 🌆 🖂 🖄 🗭 🔜 🐺 🖸	3	🌶 🔍 🖉				

2.螢幕出現如下畫面,選擇【Decrypt/Verify】。



3.出現選取檔案視窗,再選取要解密之成績檔H???.csv.gpg,點選【開啟】。

Select File(s) to Decrypt/Verify	? 🔀
搜尋位置①: 🔒 我的交件	▼ 🖷 🖆 🖛
≥H979.csv.gpg	
檔案名稱(11): H979.csv.gpg	
檔案類型(I): All Files (*.*)	▼ 取浦
	Clipboard

4. 輸入密碼(產生鑰匙對時設定的密碼)後,按【Ok】。

PGPtools - Enter Passphrase	2 🛛
Message was encrypted to the following public key(s) :	
ceeckey <exam@ceec.edu.tw> (DH/2048) key979 <test@tp.edu.tw> (DH/2049)</test@tp.edu.tw></exam@ceec.edu.tw>	
mter passphrase	✓ Hide Typing
	▼

第9頁.共10頁

5.出現下圖表示解密成功,同時在相同目錄中產生 H???.csv 成績檔。

🧳 PG Plog				×
Name	Signer	Validity	Signed	
M979.csv.pgp	ceeckey <examdp@ceec.edu.tw></examdp@ceec.edu.tw>	•	2008/9/22 下午 03:30:29	
<	Ш		3	>

註:Signer 欄中若出現 Unknown 表示未匯入大考中心「考試專用公鑰」(ceeckey. asc), 請參考前節匯入公鑰。



6.如出現下圖即表示成績檔無法開啟或成績檔被更改過。

