

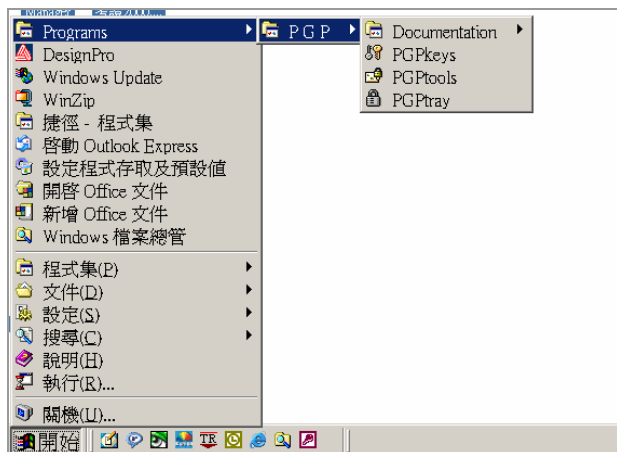
## PGP (Pretty Good Privacy Suite) 操作說明

### 一、鑰匙對製作

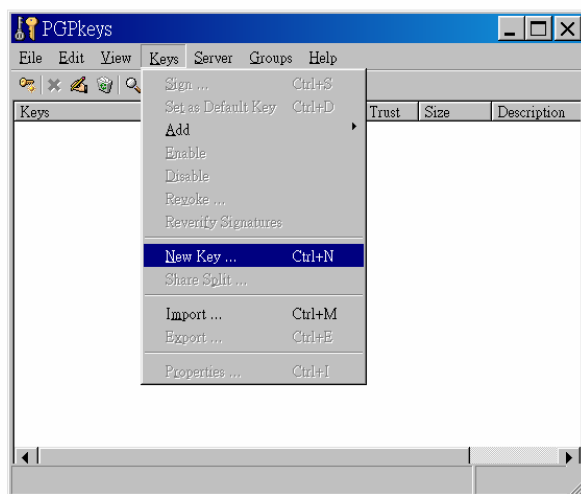
#### (一) 執行 PGP 製作鑰匙對

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

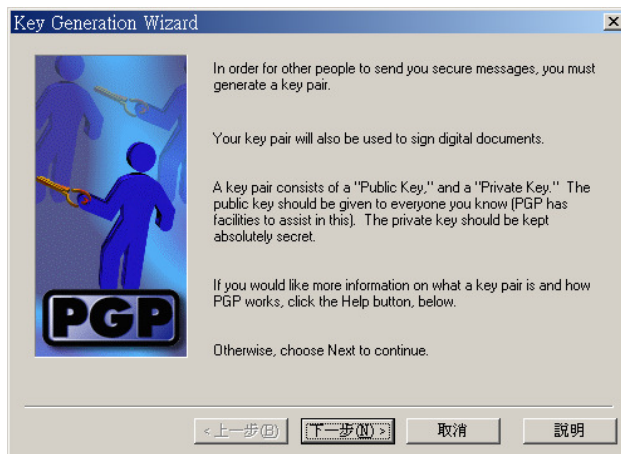
(※如點選【程式集】→【PGP】→【空】會無法開啟 PGP 請依上列方式操作)



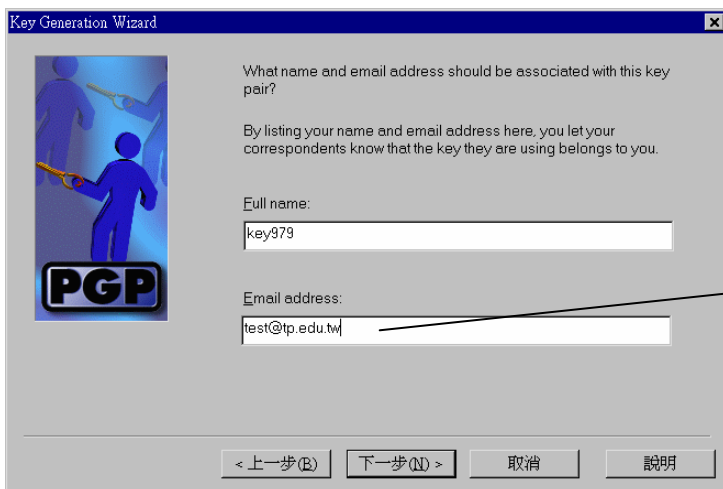
2. 產生新的鑰匙對 (先將系統中原有之預設值鑰匙對或不需用之鑰匙對刪除)。



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



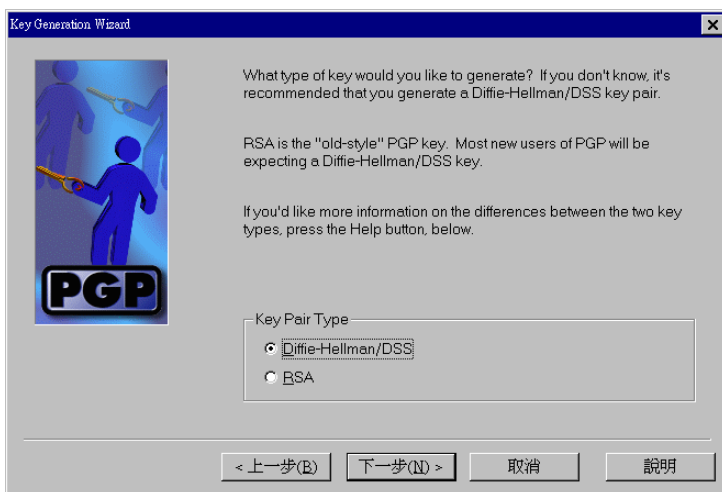
4. 輸入鑰匙對連結的 Full name 及 Email address 之後，選擇【下一步】。  
Full name 以【key???】命名 (???為單位代碼，本範例為 key979)。



The dialog box is titled "Key Generation Wizard". It contains a PGP logo on the left. The main text asks for a name and email address. The "Full name:" field contains "key979" and the "Email address:" field contains "test@tp.edu.tw". At the bottom are buttons for "< 上一步(B)", "下一步(N) >", "取消", and "說明".

報名單位在大考中心登錄之聯絡信箱

5. 點選【Diffie-Hellman/DSS】，選擇【下一步】。



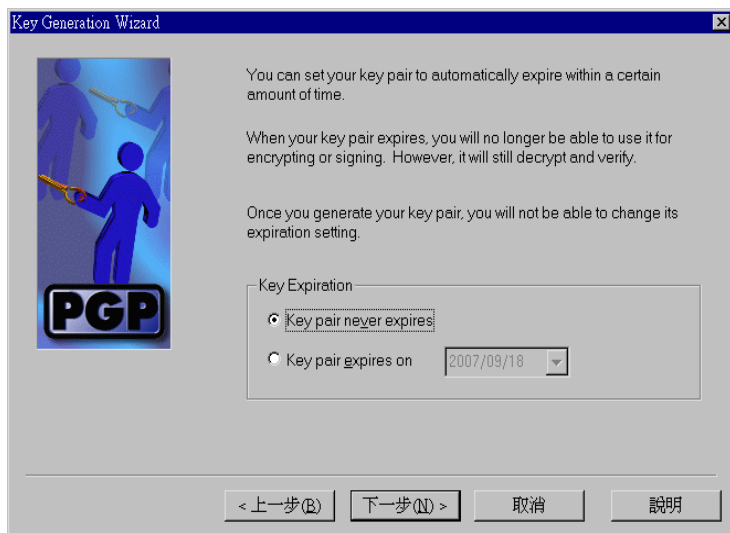
The dialog box is titled "Key Generation Wizard". It contains a PGP logo on the left. The main text asks for the type of key. The "Key Pair Type" section has two radio buttons: "Diffie-Hellman/DSS" (selected) and "RSA". At the bottom are buttons for "< 上一步(B)", "下一步(N) >", "取消", and "說明".

6. 點選【2048 bits】，選擇【下一步】。

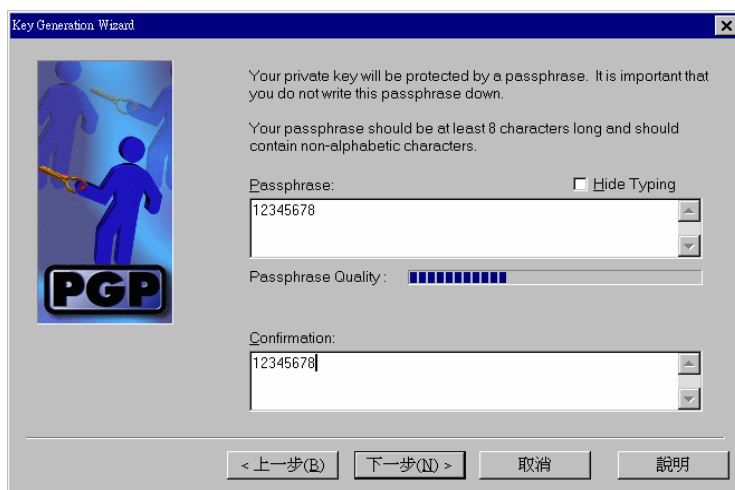


The dialog box is titled "Key Generation Wizard". It contains a PGP logo on the left. The main text asks for the size of the key pair. The "Key Pair Size" section has five radio buttons: "1024 bits", "1536 bits (1536 Diffie-Hellman/1024 DSS)", "2048 bits (2048 Diffie-Hellman/1024 DSS)" (selected), "3072 bits (3072 Diffie-Hellman/1024 DSS)", and "Custom (1024 - 4096 bits)". Below the radio buttons is a text box containing "2048". At the bottom are buttons for "< 上一步(B)", "下一步(N) >", "取消", and "說明".

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



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）

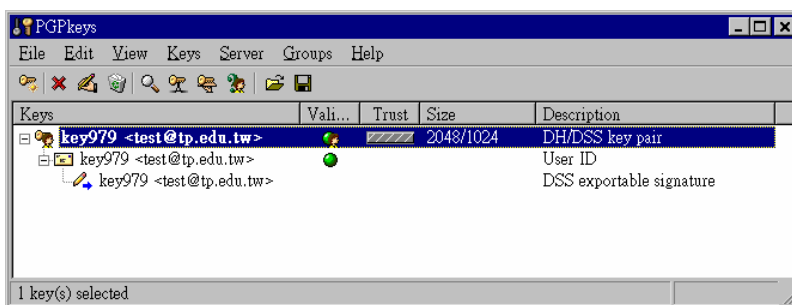


9.請依螢幕指示點選【下一步】，直至以下畫面即表示已經產生 PGP Key pair(PGP 鑰匙對)，選擇【完成】。

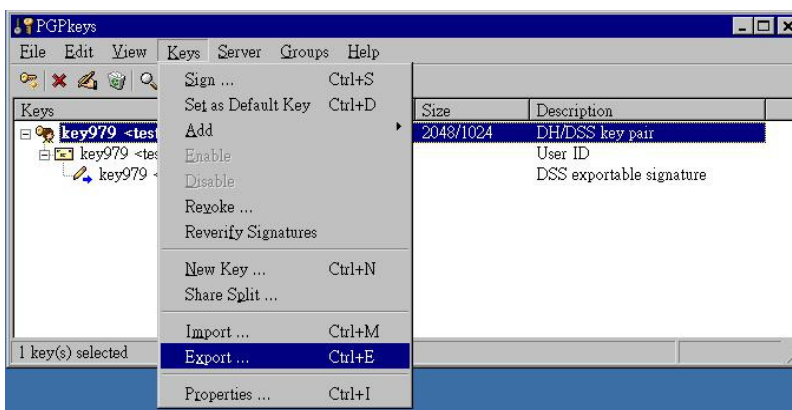


## (二) 匯出 Public Key (公鑰)

1. 選取欲匯出之鑰匙對 (如本範例 Key979)。

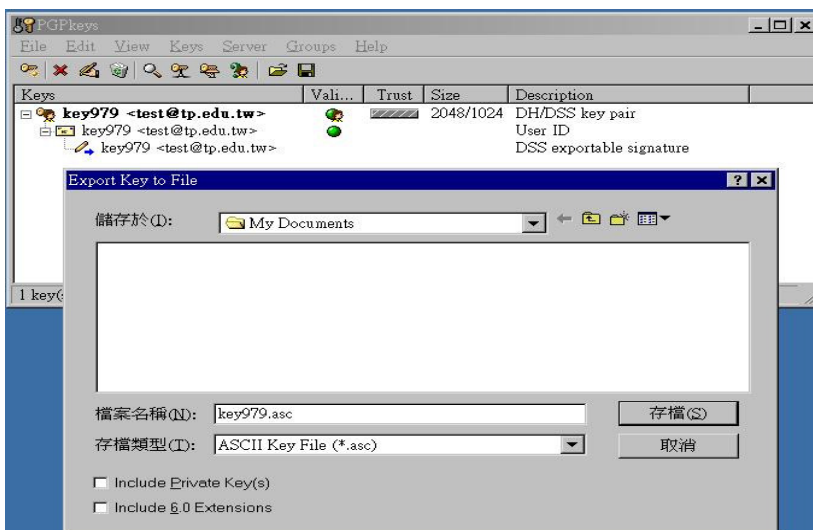


2. 點選【Keys】下拉選單，選取【Export】。



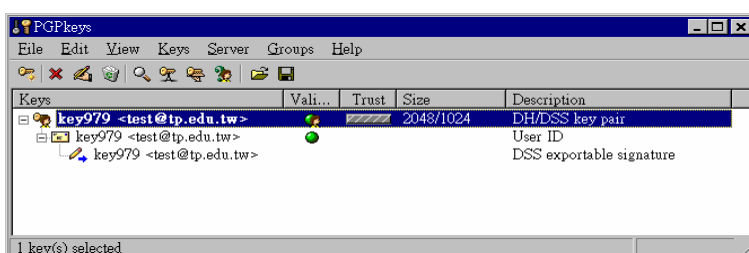
3. 選擇儲存公鑰檔的目錄(資料夾) (如本範例之公鑰檔【key979.asc】

儲存於 [My Documents] 資料夾中)，點選【存檔】即完成。

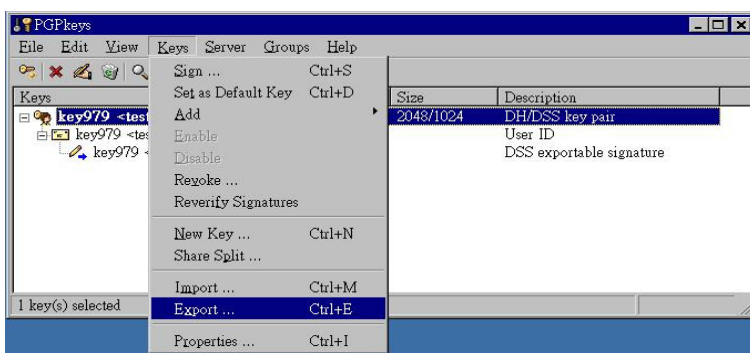


## (三) 備份鑰匙對

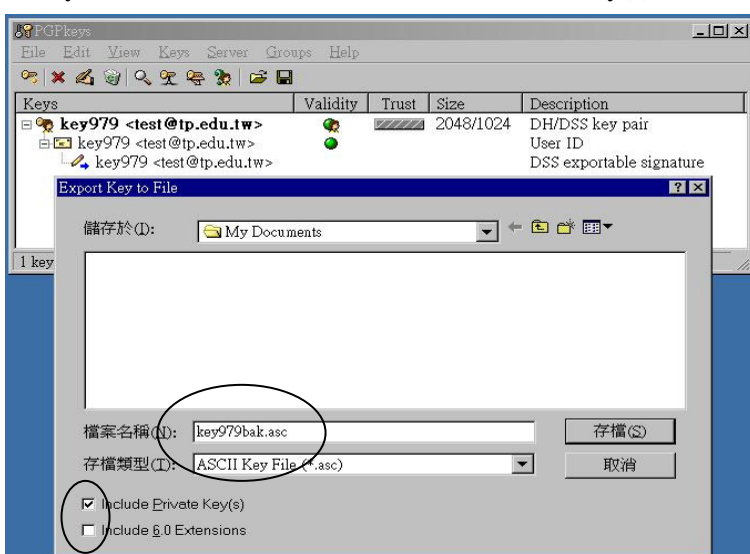
1. 點選鑰匙對 (如本範例 Key979)。



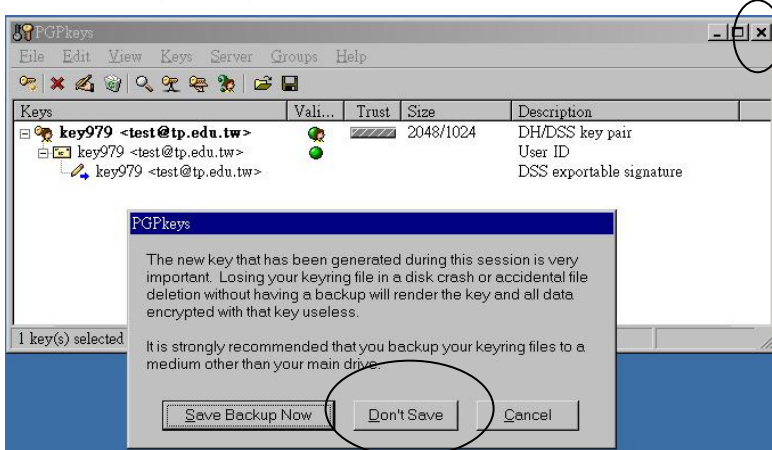
2. 點選【Keys】下拉選單，選取【Export】。



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。

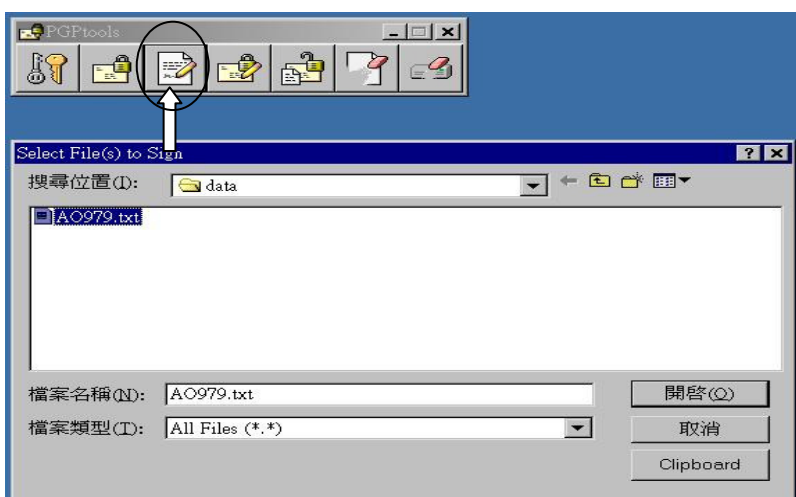


※請妥善保存備份的鑰匙對 key???.bak.asc，若原有的鑰匙對不慎遺失或更換電腦，可將此備份鑰匙對匯入使用。

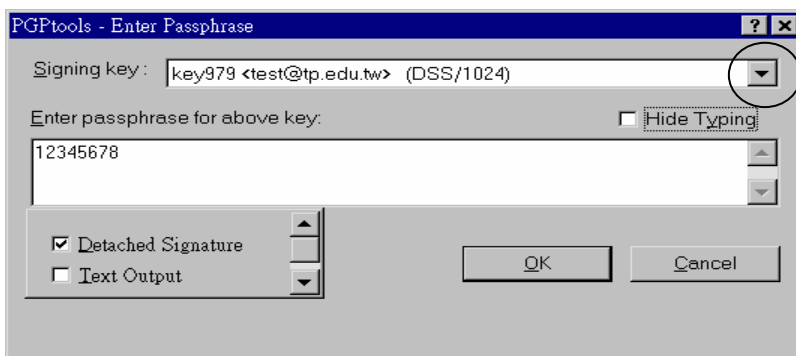
## 二、資料簽章

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 (???.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，檔案存在指定目錄下《如學測及術科為 C:\\*\*Sat\data、指考為 C:\\*\*Drse\data (\*\*為學年度)》。

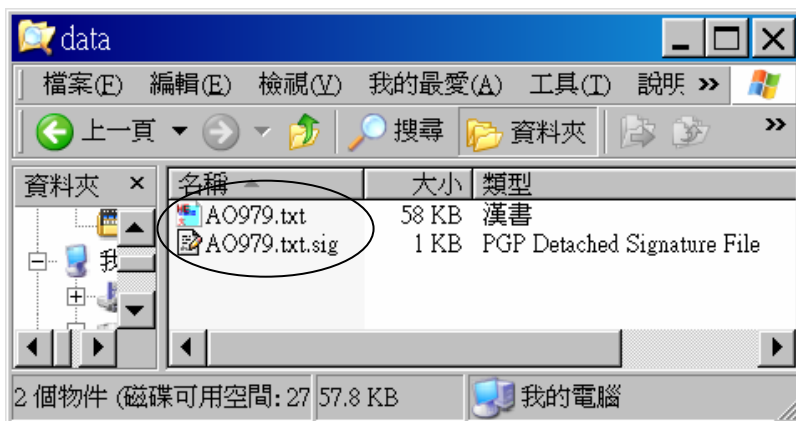
1. 開啟 PGTools，點選【Sign】(如下圖箭頭指示)出現選取檔案視窗，再選取要簽章的文件 AO???.txt，點選【開啟】。  
(亦可不開啟 PGTools，先自指定目錄下選取 AO???.txt，按滑鼠右鍵選取【PGP】→選取【Sign】，直接進入下個步驟畫面)



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)



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)。



### 三、資料驗證

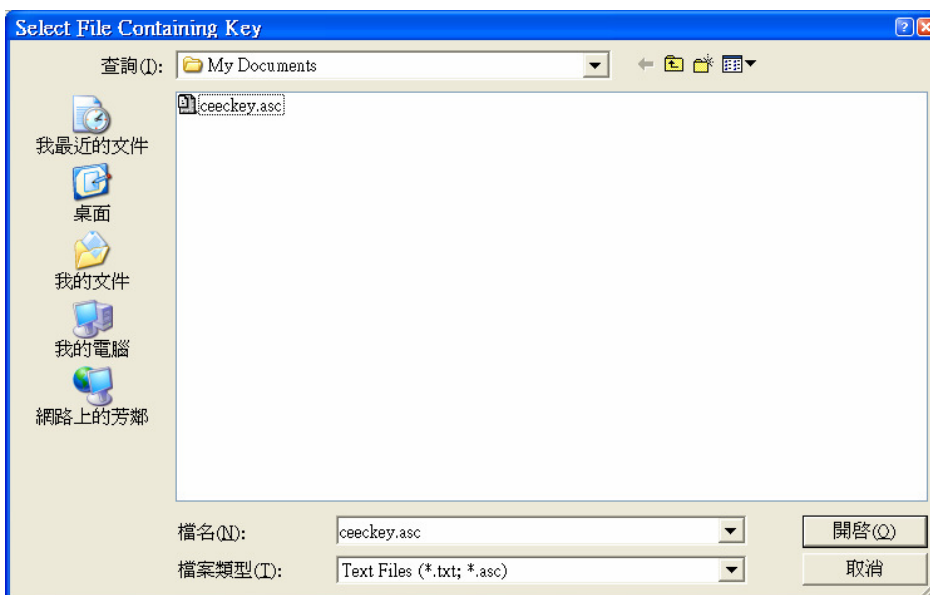
本中心傳送各項試務資料檔案（如准考證清冊及試場分配表檔案）及成績檔時，均使用電子簽章，各報名單位須使用本中心「**考試專用公鑰**」（以 ceec?.asc 命名，??為西元年度，例 ceec2011.asc）來核驗並確認檔案。請洽本中心第二處取得本中心公鑰，並將其匯入貴單位之簽章軟體內。

#### (一)匯入大考中心「**考試專用公鑰**」（下列說明以 ceeckey.asc 為例）

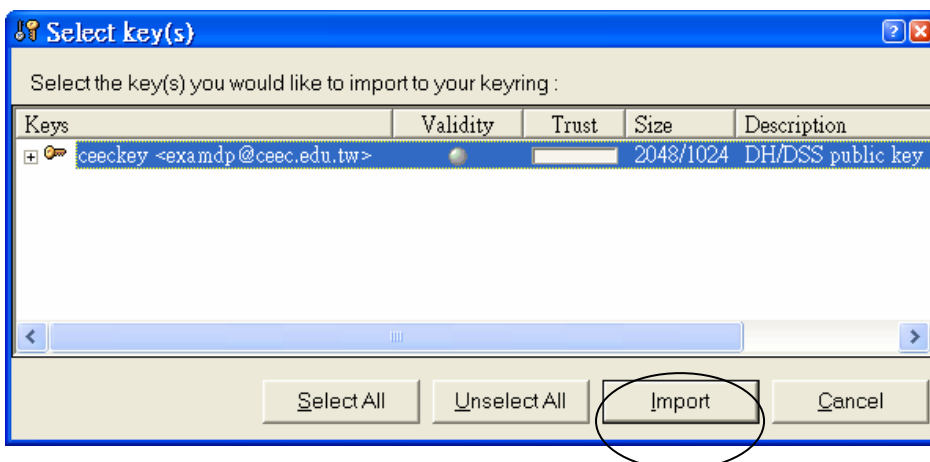
1.開啟【PGPkeys】，點選【Keys】下拉選單，點選【Import】。



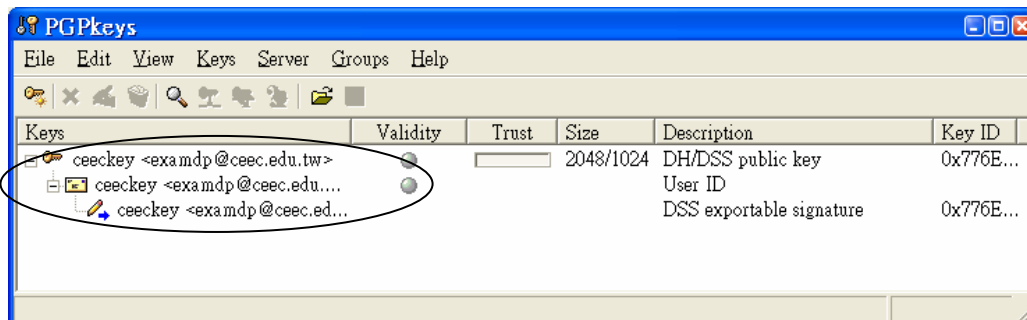
2.出現選取檔案視窗，選取 ceeckey.asc，點選【開啟】。



3.點選【Import】。



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



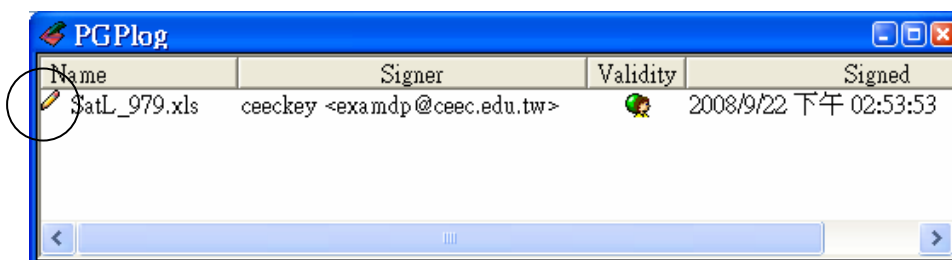
## (二) 檢查資料檔是否被更改

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

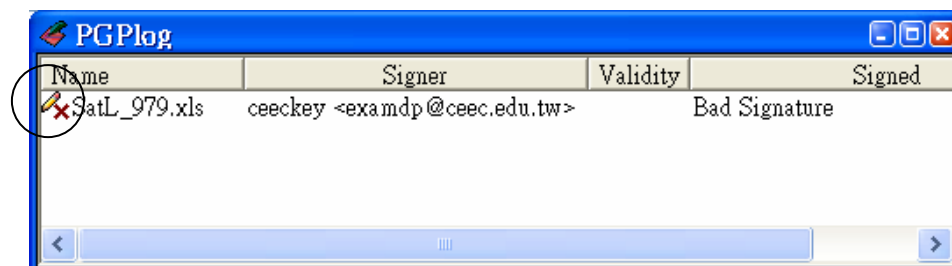
開啟簽章檔【SatL\_979.xls.sig】(double click)，

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



圖二 若資料檔被更改過，則簽章檔會出現「×」

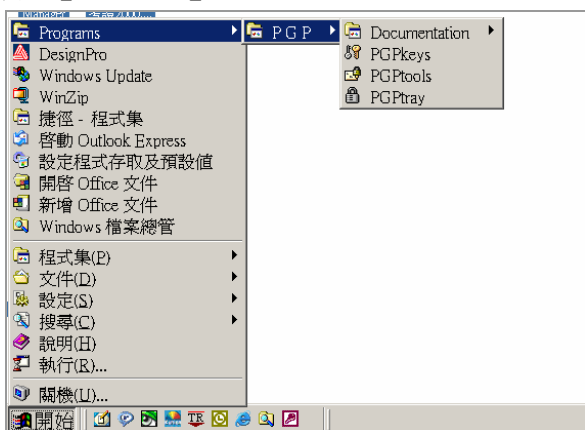




#### 四、資料解密方式

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：

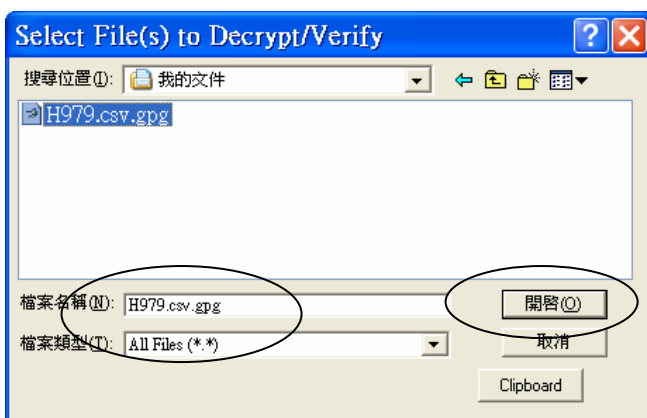
1.點選【PGPtools】。



2.螢幕出現如下畫面，選擇【Decrypt/Verify】。



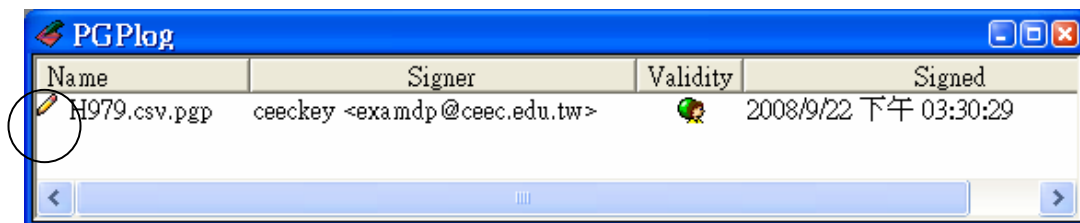
3.出現選取檔案視窗，再選取要解密之成績檔 H???.csv.gpg，點選【開啟】。



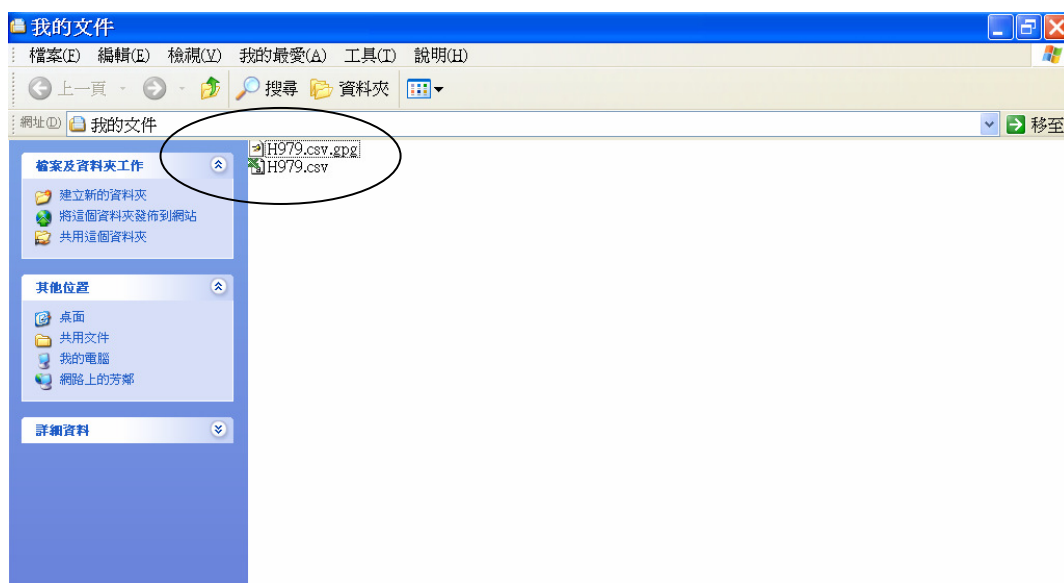
4.輸入密碼（產生鑰匙對時設定的密碼）後，按【Ok】。



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。



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。

