

JUN 11 TUE 2013 12:25

GnuPG (GPG) In Win32 免費檔案加解密軟體概念與實作

分享:       6

當商業檔案如 EDI (850,860,810...) 在 FTP 協定中傳輸時，若被別人截取，那資料就會外洩。若能在傳輸前先加密，到客戶端時再作解密，這就保險多了。檔案加解密的軟體很，GnuPG (GPG) 是一套完全免費的軟體(GnuPG is the [GNU project's complete and free implementation of the OpenPGP standard as defined by RFC4880](#))，也有在實務的商務中使用，安全性很高值得一用。

GnuPG 概念：

GPG, like PGP (Pretty Good Privacy), uses a key pair. This means that when you generate a key, you will create a public copy as well as private copy. The private copy is your copy used to decrypt an incoming file as well sign an outgoing file (but for our purposes, we are only using it to decrypt). The public key is the key you give to the public, which is used to encrypt the files coming to you. First we will create your own key.

These keys are stored in key rings. For GPG, they are stored in the directory that the GPG files were copied into. They are both named with a .GPG extension, and are called **pubring.GPG** and **secring.GPG** (to denote the public key ring and the private key ring, respectively).

原文的意思主要是說：GPG 會產生一組 Key，一個是私鑰 (Private Key:**secring.GPG**) 用來解碼檔案，以及傳出檔案時作簽章 (sign)；一個是公鑰 (Public Key:**pubring.GPG**) 是要給客戶的，當客戶要傳檔案給你時，用此公鑰作加密。兩個檔案都是以 .GPG 作為附檔名。

Google Search 站內文章搜尋

Google™ Custom Search

Search

我的連結

[我與小歲歲的工作日記](#)[我與小歲歲的生活日記](#)[我與小歲歲的電影日記](#)[MISTECH 技術手抄本在 Xuite 隨意窩](#)

熱門文章

[\(27144\)Windows 安裝 Apache 2.2 + MySQL 5.6 + PHP 5.4 教學](#)[\(10255\)Linux 檔案格式 ext2 ext3 ext4 比較](#)[\(10196\)Apache - VirtualHost 架設虛擬網站](#)[\(7465\)Maven 的基本概念與在 eclipse 專案實作](#)[\(6966\)Oracle RMAN 的基本概念與資料庫全備份實作](#)

線上人數

 3

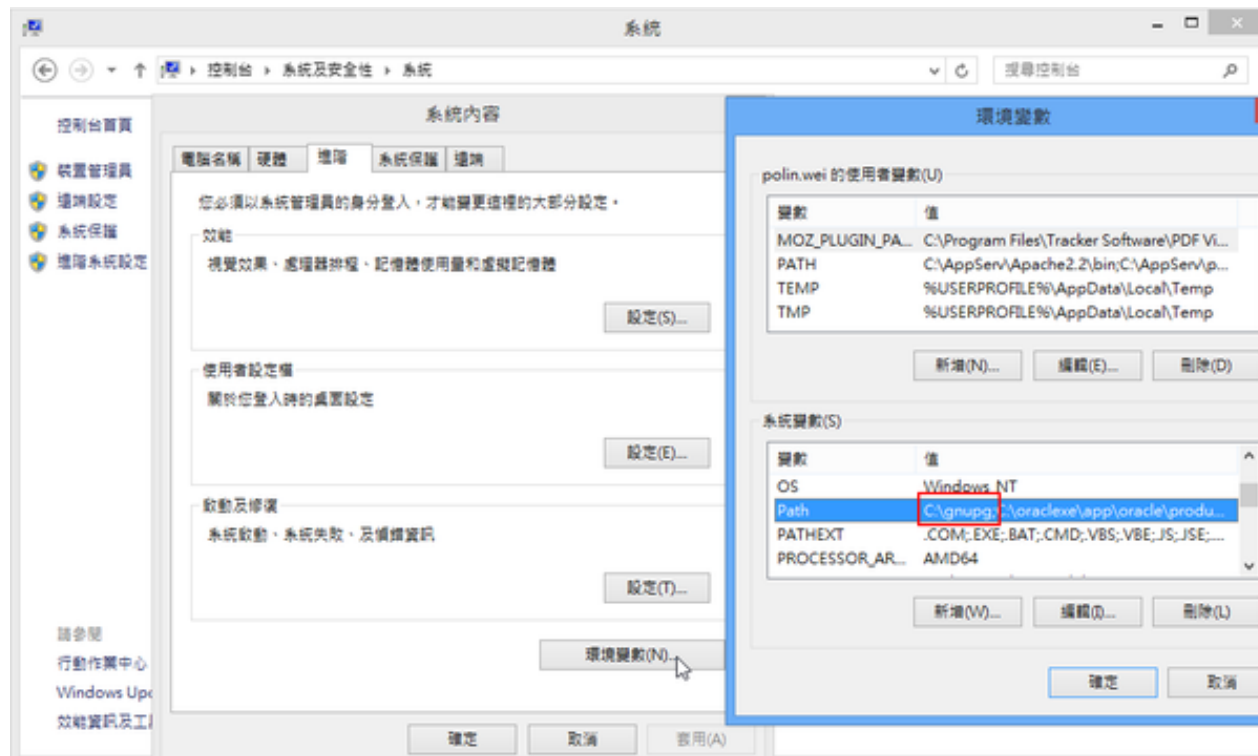
GnuPG 實作：

那要如何建立這一組Key：私鑰 (Private Key:**secring.GPG**)& 公鑰 (Public Key:**pubring.GPG**)，下面一個步驟一個步驟來作解說：

step 01: 環境設定

先到 GnuPG 的下載網站：下載軟體 [gnupg-w32cli-1.2.0.zip](http://ftp.gnupg.org/GnuPG/binary/gnupg-w32cli-1.2.0.zip).
([ftp://ftp.gnupg.org/GnuPG/binary/gnupg-w32cli-1.2.0.zip](http://ftp.gnupg.org/GnuPG/binary/gnupg-w32cli-1.2.0.zip))，這裡使用gnupg-w32cli-1.2.0 版。在 Windows 平台，可以用 7Z 解壓，並將解開的目錄放在 C:\gnupg

再到 開始(Start) > 控制(Control Panel) > 系統(System). 選擇 進階(Advanced tab) 並編輯環境變數中的 Path 參數。



step 02: 產生私鑰 (Private Key:**secring.GPG**)& 公鑰 (Public Key:**pubring.GPG**)

```
C:\gnupg> c:\gnupg\gpg --gen-key
gpg (GnuPG) 1.2.0; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
```



參觀人氣

本日人氣：180

累積人氣：130799

文章分類

- + PTC-Windchill (1)
- + Server (6)
- + Java (4)
- + Oracle EBS (6)
- + PL/SQL (1)
- + DataBase (2)
- + PHP (1)
- + HTML (2)
- + JavaScript (1)
- + XOOPS (3)
- + Linux (1)
- [未分類文章 \(1\)](#)

BloggerAds



This is free software, and you are welcome to redistribute it under certain conditions. See the file COPYING for details.

gpg: keyring `c:/gnupg\secreing.gpg' created

gpg: keyring `c:/gnupg\pubring.gpg' created

Please select what kind of key you want:

(1) DSA and ElGamal (default) <= 選擇預設即可

(2) DSA (sign only)

(5) RSA (sign only)

Your selection?

DSA keypair will have 1024 bits.

About to generate a new ELG-E keypair.

minimum keysize is 768 bits

default keysize is 1024 bits

highest suggested keysize is 2048 bits

What keysize do you want? (1024) **2048** <= 輸入 2048

Requested keysize is 2048 bits

Please specify how long the key should be valid.

0 = key does not expire

<n> = key expires in n days

<n>w = key expires in n weeks

<n>m = key expires in n months

<n>y = key expires in n years

Key is valid for? (0) **10y** <= 有效時間10年, 若為0則不失效

Key expires at 06/09/23 10:01:10

Is this correct (y/n)? **y** <=輸入y表示正確無誤

You need a User-ID to identify your key; the software constructs the user id from Real Name, Comment and Email Address in this form:

"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: **polin.wei** <=這是 USER-ID 作加/解密時要指定用的

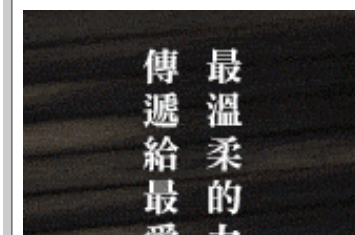
Email address: **polin.wei@xxx.com**

Comment:

You selected this USER-ID:

"**polin.wei** <**polin.wei@xxx.com**>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? **o** <=確定輸入 o



Secret key is available.

```
gpg: checking the trustdb
gpg: checking at depth 0 signed=0 ot(-/q/n/m/f/u)=0/0/0/0/0/1
gpg: next trustdb check due at 2023-06-09
pub 1024D/FBA68168 created: 2013-06-11 expires: 2023-06-09 trust: u/u
sub 2048g/9E6074F7 created: 2013-06-11 expires: 2023-06-09
(1). polin.wei <polin.wei@xxx.com>
```

Command> **passwd**

Key is protected.

//先輸入原來的密碼

You need a passphrase to unlock the secret key for

user: "**polin.wei <polin.wei@xxx.com>**"

1024-bit DSA key, ID 53FA0BBC, created 2013-05-23

/**再輸入新的密碼，若連續按兩次 Enter 鍵，則密碼為空，系統會告知this is
probably a *bad* idea! **/

Enter the new passphrase for this secret key.

You don't want a passphrase - this is probably a *bad* idea!

Do you really want to do this? yes

step 03: 匯出要給客戶的公鑰

利用 step 02 最後的資訊(如下)來匯出要給客戶的公鑰

/** 下面是這一組Key的資訊 **/

```
pub 1024D/FBA68168 2013-06-11 polin.wei <polin.wei@xxx.com>
    Key fingerprint = 925A 54A5 03DA 5CFD ECE5 F01C A5DC 98A3 FBA6
8168
sub 2048g/9E6074F7 2013-06-11 [expires: 2023-06-09] <=用這一組來指定
9E6074F7 匯出公鑰
```

C:\gnupg>**gpg --export --output polinwei.asc 9E6074F7**

urlad



這時會匯出一個檔名為 **polinwei.asc** 的公鑰，這就是要給客戶匯入用的；當然，客戶也會給你他的公鑰，你也必需匯入進來，並作信認 (Trust)

step 04: 匯入客戶的金鑰(**partnerid.asc** 此為範例檔)，並信認(Trust)

C:\gnupg>gpg --import partnerid.asc <=匯入客戶的金鑰

```
gpg: key 55FA0BBC: public key "Partner <edi.admin@Partner.com>" imported
gpg: Total number processed: 1
gpg:             imported: 1
```

C:\gnupg>gpg --edit-key 55FA0BBC <=指定要維護那一間客戶

```
gpg (GnuPG) 1.2.0; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.
```

```
gpg: checking the trustdb
gpg: checking at depth 0 signed=0 ot(-/q/n/m/f/u)=0/0/0/0/0/1
gpg: next trustdb check due at 2023-06-09
pub 1024D/55FA0BBC created: 2013-05-23 expires: 2023-05-21 trust: -/-
sub 2048g/DD28189F created: 2013-05-23 expires: 2023-05-21
(1). Partner <edi.admin@Partner.com>
```

Command> **trust** <= 對此客戶作信認

```
pub 1024D/55FA0BBC created: 2013-05-23 expires: 2023-05-21 trust: -/-
sub 2048g/DD28189F created: 2013-05-23 expires: 2023-05-21
(1). Partner <edi.admin@Partner.com>
```

Please decide how far you trust this user to correctly
verify other users' keys (by looking at passports,
checking fingerprints from different sources...)?

- 1 = Don't know
- 2 = I do NOT trust
- 3 = I trust marginally
- 4 = I trust fully

個人資訊



加入好友

加入訂閱

暱稱：MIS

分類：圖文創作

好友：共4位 (看全部)

地區：台中市

5 = I trust ultimately
m = back to the main menu

Your decision? **5** <= 選擇 5

Do you really want to set this key to ultimate trust? yes

```
pub 1024D/55FA0BBC created: 2013-05-23 expires: 2023-05-21 trust: u/-
sub 2048g/DD28189F created: 2013-05-23 expires: 2023-05-21
(1). Partner <edi.admin@Partner.com>
Please note that the shown key validity is not necessarily correct
unless you restart the program.
```

Command> **quit** <= 離開

step 05: 檢查客戶的公鑰是否正確存在

```
C:\gnupg>gpg --list-keys
c:/gnupg/pubring.gpg
-----
pub 1024D/FBA68168 2013-06-11 polin.wei <polin.wei@xxx.com>
sub 2048g/9E6074F7 2013-06-11 [expires: 2023-06-09]

pub 1024D/55FA0BBC 2013-05-23 Partner <edi.admin@Partner.com>
sub 2048g/DD28189F 2013-05-23 [expires: 2023-05-21]
```

以上的步驟就是產生一組私鑰 (Private Key:**secring.GPG**)& 公鑰 (Public Key:**pubring.GPG**)，與匯出公鑰 polinwei.asc 及匯入客戶公鑰 **partnerid.asc** 的完整過程。

 **GPG**, **GnuPG**, **Private Key**, **secring.GPG**, **Public Key**, **pubring.GPG**

MIS 發表在 痞客邦 PIXNET 留言(0) 人氣(1176)

[E-mail轉寄](#) [轉寄至留言板](#)

最新留言

09/19 訪客：

[可以](#)

09/11 Fen Fan：

[請問 Window sever: \(2003\) ...](#)

08/26 志峰 李：

[EBS版本:R12.2 HI...你好,...](#)

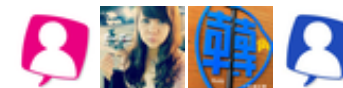
12/17 版主回覆：

[應該是這個存放 ssl 憑證的目...](#)

12/15 訪客：

[您好 我想請問 目前是照您...](#)

我的好友



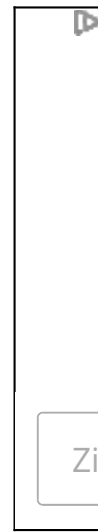
顯示共 4 名好友

誰來我家



博客來 AP





全站分類： [進修深造](#)

個人分類： [HTML - SSL](#)

此分類上一篇： [Certificate Authority\(CA\) 憑證的運用簡介](#)

此分類下一篇： [GnuPG \(GPG\) In Win32 免費檔案加解密軟體的運用](#)

上一篇： [Ajax - XMLHttpRequest 物件的一些基本方法](#)

下一篇： [GnuPG \(GPG\) In Win32 免費檔案加解密軟體的運用](#)

歷史上的今天

2015: [Extending partitions in Windows using DiskPart 擴展磁碟空間：Extend Data Volume on a Windows 2003 Virtual Machine \(VMware ESXi\)](#)

2015: [VMware Esxi:Disk Consolidation Needed - Unable to access file since it is locked](#)

2013: [GnuPG \(GPG\) In Win32 免費檔案加解密軟體的運用](#)

▲TOP

留言列表 (0)

發表留言

PIXNET Facebook Yahoo! Google MSN/Live


推 0

您尚未登入，將以訪客身份留言。亦可以上方服務帳號登入留言

您的暱稱 ...

留個言吧 ...

☐ 悄悄話

 其他選項

送出留言