

電子發票整合服務平台 加解密 API 使用說明書

版本：1.12

財政部財政資訊中心

中華民國 105 年 11 月

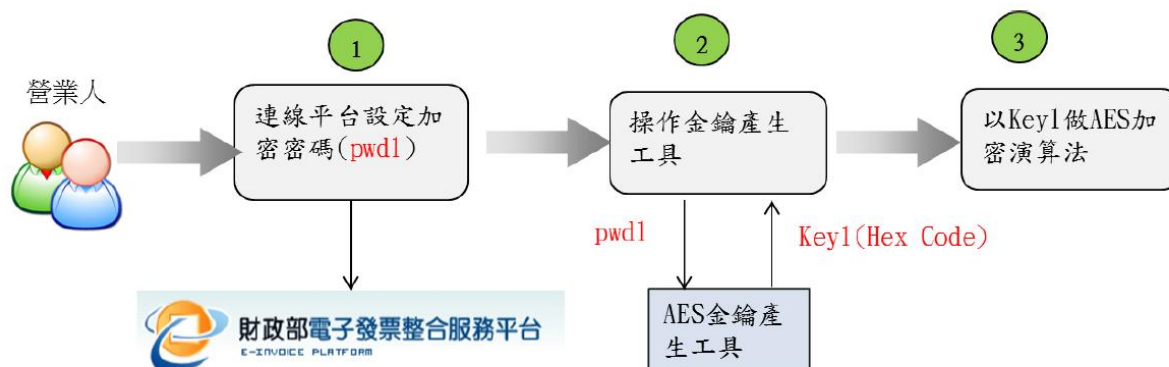
修訂表：

版本	制／ 修訂 人員	變更內容摘要	頁數	提供日期
V1.0	葉浚豪	初版制訂。	A11	100.11.16
V1.1	葉浚豪	說明QR Code DLL API。	P2~P4	100.11.29
V1.2	葉浚豪	修正[貳、二產生QR Code字串API說明]介面描述。	P2~P3	100.12.01
V1.3	葉浚豪	1. 連線平台設定加密密碼說明 2. 修 改 欄 位 ProductQty/ProductSaleAmount/ProductAmount/ProductTaxAmount型態為字串。	P1~P3 P5	100.12.05
V1.4	葉浚豪	1. 新增C版本API, 範例, 錯誤代碼檔 2. .NET版本加入輸入判斷 3. 增加相關工具說明	P6~P8 P5 P10~P12	100.12.19
V1.5	葉浚豪	1. 新增中獎清冊下載作業說明 2. 並調整相關工具的章節	P10	101.01.17
V1.6	葉浚豪	1. 說明JDK版本	P16	101.03.16
V1.7	陳俊光	1. 新增QRCode 線上解密驗證步驟	P9~P11	101.04.02
V1.8	陳俊光 林毓棠	1. 增加發票檢核說明 2. 發票機敏欄位加密使用說明	P4~P6 P12	101.04.20 101.04.26
V1.9	陳俊良	1. 修改傳輸參數，取消二維商品資料陣列 2. 更新範例程式內容	P5 P6~8	101.07.20
V1.10	陳俊良	1. 修正銷售額可以為0	P4、P5	101.09.27
V1.11	莊棠鈞	內容全面檢視並調整	P1~P23	105.07.27
V1.12	潘怡君	修訂第貳章QRCode相關內容說明	P6~P11	105.11.15

目錄

壹、 加密機制說明	1
一、 連線平台設定加密密碼說明	2
貳、 QR Code	6
一、 QR Code 字串 API 使用說明	6
二、 QR Code 字串說明	6
三、 產生 QR Code 字串 API 說明	7
四、 QR Code 字串 API 範例(.NET 及 C)	8
五、 QR Code 線上解密驗證	11
參、 發票機敏欄位加密	14
一、 API 使用說明	14
二、 API 介面說明	14
三、 API 範例(.NET)	14
肆、 下載中獎清冊	16
一、 UI Mode 執行方式	16
二、 Command Mode 執行方式	20
伍、 其他相關工具	23
一、 產生加密金鑰 (genKey.bat/genKey.sh)	23

壹、 加密機制說明

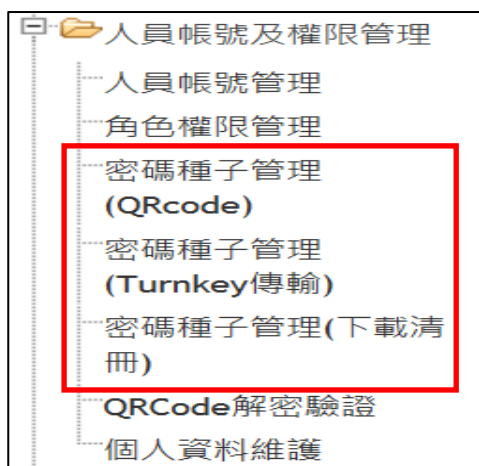


上圖為加解密機制流程，賣方或總機構營業人管理者需登入電子發票整合服務平台設定加密密碼，設定完成後營業人在營業人端並將此組密碼透過AES金鑰產生工具(請參考章節[伍、一、產生加密金鑰 (genKey.bat/genKey.sh)])產生出賣方或總機構營業人加密金鑰。並以此金鑰做為AES加密演算法來加密資料。此做法能確保每家營業人管理自己的金鑰，並透過公開AES加密演算法來確保資料的安全性。

加密機制會使用在三個地方，分別為電子發票證明聯 QR Code 產生、發票機敏欄位加密、中獎清冊加密機制。營業人在電子發票整合服務平台設定加密密碼，可對此三種應用分別設定不同之加密密碼，說明如下。

一、連線平台設定加密密碼說明

使用者以管理員身份登入電子發票整合服務平台後可選擇 3 種「密碼種子管理」進行設定，以下將分別針對 3 種密碼種子說明。



(一) 密碼及種子管理(QRCode)

QR Code 密碼種子係用於賣方營業人產製電子發票證明聯之加密驗證資訊，詳細內容可參考章節「貳、QR Code」，營業人設定 QR Code 密碼種子可選擇以「憑證」或「密碼種子」登入。

1. 以憑證登入密碼及種子管理(QRCode)

現在位置 / 人員帳號與權限管理 > 密碼及種子管理(QRcode) > 授權確認

授權確認

統一編號

00007104

✓

登入確認方式

☒ 憑證登入 ☐ 密碼種子登入

憑證種類

工商憑證

▼

卡片密碼

✓

※請插入憑證並輸入pin碼後按下[授權確認]登入

2. 以密碼種子登入方式設定 QR Code 密碼種子

現在位置 / [人員帳號與權限管理](#) > [密碼及種子管理\(QRcode\)](#) > 授權確認

授權確認

統一編號	<input type="text" value="00007104"/>	✓
登入確認方式	<input type="radio"/> 憑證登入 <input checked="" type="radio"/> 密碼種子登入	
密碼種子密碼	<input type="text"/>	✓

※請輸入您的密碼種子並按下[授權確認]登入，如果是您第一次設定此密碼，密碼欄位請留空白才能登入。

 授權確認

(二) 密碼及種子管理(Turnkey 傳輸)

Turnkey 傳輸密碼種子係提供營業人將包含敏感資料(如：信用卡卡號、金融卡)發票資料進行加密，詳細內容可參考章節「參、發票機敏欄位加密」，營業人設定 Turnkey 傳輸密碼種子可選擇以「憑證」或「密碼種子」登入。

1. 以憑證登入密碼及種子管理(Turnkey 傳輸)

現在位置 / [人員帳號與權限管理](#) > [密碼及種子管理\(TurnKey傳輸\)](#) > 授權確認

授權確認

統一編號	<input type="text" value="00007104"/>	✓
登入確認方式	<input checked="" type="radio"/> 憑證登入 <input type="radio"/> 密碼種子登入	
憑證種類	<input type="text" value="工商憑證"/>	▼
卡片密碼	<input type="text"/>	✓


※請插入憑證並輸入pin碼後按下[授權確認]登入

 授權確認

2. 以密碼種子登入密碼及種子管理(Turnkey 傳輸)

現在位置 / [人員帳號與權限管理](#) > [密碼及種子管理\(TurnKey傳輸\)](#) > 授權確認


授權確認

統一編號 00007104 

登入確認方式 ☐ 憑證登入 ☒ 密碼種子登入

密碼種子密碼 

※請輸入您的密碼種子並按下[授權確認]登入，如果您第一次設定此密碼，密碼欄位請留空白才能登入。

 授權確認


(三) 密碼及種子管理(下載清冊)

本功能係提供營業人下載種獎清冊使用，詳細內容可參考章節「參、發票機敏欄位加密」，營業人設定下載清冊之密碼種子可選擇以「憑證」或「密碼種子」登入。


1. 以憑證登入密碼及種子管理(下載清冊)

現在位置 / [人員帳號與權限管理](#) > [密碼及種子管理\(下載清冊\)](#) > 授權確認

授權確認


統一編號 00007104 

登入確認方式 ☒ 憑證登入 ☐ 密碼種子登入

憑證種類 工商憑證 

卡片密碼 

※請插入憑證並輸入pin碼後按下[授權確認]登入

 授權確認


2. 密碼及種子管理(下載清冊)密碼種子登入方式設定

▶ 現在位置 / [人員帳號與權限管理](#) > [密碼及種子管理\(下載清冊\)](#) > 授權確認

授權確認

統一編號	<input type="text" value="00007104"/>	✓
登入確認方式	<input type="radio"/> 憑證登入 <input checked="" type="radio"/> 密碼種子登入	
密碼種子密碼	<input type="text"/>	✓

※請輸入您的密碼種子並按下[授權確認]登入，如果您第一次設定此密碼，密碼欄位請留空白才能登入。

 授權確認

貳、QR Code

營業人在產生 QR Code 字串，可以依照 QR Code 規格來自行產製字串，或使用電子發票整合服務平台所提供之 API 來產生前 77 碼 QR Code 字串，有關 QR Code 字串規格請參考[電子發票證明聯一維及二維條碼規格說明]文件。

建議營業人電子發票整合服務平台所提供 API 來產生 QR Code，以利未來 QR Code 規範更新時，只須更新電子發票整合服務平台所提供之 API 即可。

電子發票整合服務平台提供 API 有 C 及 .Net 兩種版本。

一、QR Code 字串 API 使用說明

當營業人使用電子發票整合服務平台所提供之 API 時，須先使用[產生加密金鑰]工具(請參考第伍章)來產生加密金鑰。金鑰將以 Hex(16 進制)呈現，使用將此字串和發票相關資訊當作輸入參數帶入 API 中，即可得到 QR Code 字串。

二、QR Code 字串說明

目前經過程式處理後產生 QR Code 字串，長度為77 碼，其字串內文依序所填入資訊為：

發票字軌(10碼)--兩位英文字母+八位數字

發票開立日期(年月日)(7碼)

四位隨機碼(4碼)--四位英數字

銷售額(8碼)--大於等於0

總計金額(8碼)- 大於0

發票買方統一編號(8碼)- 買受人為一般消費者時，填00000000

發票開立賣方統一編號(8碼)- 即銷售店統一編號

加密驗證資訊(24 碼)

電子發票證明聯中的 QR Code，第二層資訊防偽只使用前面 77 碼，後面為產品明細等資訊不參與 AES 加密。

三、產生 QR Code 字串 API 說明

API 介面為使未來 QR Code 字串規格更新時，營業人只需更換 DLL 檔仍可繼續使用API，故API介面在設計時要求將發票中有的所有資訊均需輸入(雖然有些欄位在當下的版本尚未用到)，也期望營業人在呼叫時能將欄位資料全都帶入。

介面描述如下：

英文名稱	中文名稱	類別	欄位必要性	備註
InvoiceNumber	發票字軌號碼	字串	M	
InvoiceDate	開立年月日 (yyymmdd)	字串	M	
InvoiceTime	時間(hhmmss)	字串	M	
RandomNumber	四位隨機碼	字串	M	
SalesAmount	銷售額	整數	M	
TaxAmount	稅額	整數	M	
TotalAmount	總計	整數	M	
BuyerIdentifier	買受人統編	字串	M	
RepresentIdentifier	代表店統編	字串	M	目前QR Code字串已不使用代表店，請直接輸入00000000
SellerIdentifier	銷售店統編	字串	M	
BusinessIdentifier	總公司統編	字串	M	如無總公司，請輸入銷售店統編
AESKey	加解密金鑰	字串(HEX)	M	
errorCode	錯誤代碼	整數	1.C版本API須要輸入)。 2.NET版本則丟出Exception。	
		代碼描述 0:檢查通過 -1:發票號碼長度不為十碼 -2:發票日期長度不為七碼 -3:發票時間長度不為六碼 -4:隨機碼長度不為四碼		

		-5:銷售額數字小於零 -6:稅額數字小於零 -7:總額數字小於等於零 -8:買受人統編長度不為八碼 -9:代表店統編長度不為八碼 -10:開立店統編長度不為八碼 -11:營業人統編長度不為八碼
--	--	---

四、QR Code 字串 API 範例(.NET 及 C)

(一) QR Code 字串 API 範例(.NET)

加解密程式範例如下，完整範例可以參考壓縮檔中 sample/net/QRCode_Sample.cs

```

1  using System;
2  using System.Collections.Generic;
3  using System.Text;
4
5  namespace QREncrypter
6  {
7      class Sample
8      {
9          static void Main(string[] args)
10         {
11             com.tradevan.qrutil.QREncrypter qrEncrypter = new
12             com.tradevan.qrutil.QREncrypter();
13             try
14             {
15                 String [][] abc=new String[1][];
16                 String result = qrEncrypter.QRCodeINV("AA12345678", "1001231", "150000",
17                 "1234", 100, 100, 100, "12345678", "87654321", "12344321", "43211234",
18                 "05D4A324ABAF4A570E64E572221E438B");
19             }
20             catch (Exception e)
21             {
22                 Console.WriteLine(e.Message);

```

23	<pre> } Console.ReadLine(); } } } </pre>
----	--

(二) QR Code 字串 API 範例(C)

加解密程式範例如下，完整範例可以參考壓縮檔中 sample/C/testAES.c

1	#include "stdafx.h"
2	#include <stdio.h>
3	#include <stdlib.h>
4	#include <tchar.h>
5	#include <windows.h>
6	
7	typedef void (__stdcall CALLBACK* LPFNDLLFUNC1)(char* InvoiceNumber, char*
8	InvoiceDate, char* InvoiceTime, char* RandomNumber, double SalesAmount, double
9	TaxAmount, double TotalAmount, char* BuyerIdentifier, char* RepresentIdentifier,
10	char* SellerIdentifier, char* BusinessIdentifier, char*** productArray, char*
11	AESKey, char *output, int *errorCode);
12	typedef void (__stdcall CALLBACK* LPFNDLLFUNC2)(char *cipherText, char *key, char
13	*out);
14	
15	LPFNDLLFUNC1 QRCodeINV; // Function pointer
16	LPFNDLLFUNC2 Encrypt; // Function pointer
17	
18	
19	int main(int argc, char* argv[])

20	{
21	HINSTANCE hInst = LoadLibrary(_T("QRDLL.dll"));
22	int rc;
23	char out[78];
24	char ***array;
25	int *errorCode;
26	array=(char ***)malloc(5);
27	errorCode=(int *)malloc(sizeof(int));
28	
29	if(hInst)
30	{
31	// Encrypt= GetProcAddress(hInst,"Encrypt");
32	QRCodeINV = GetProcAddress(hInst,"QRCodeINV");
33	if (!QRCodeINV)
34	{
35	

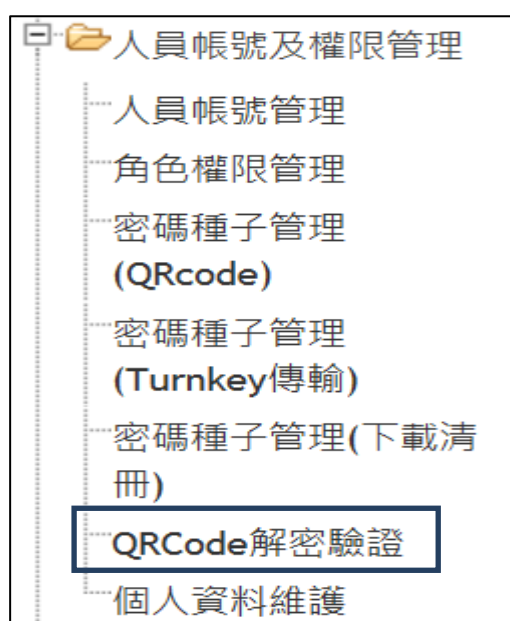
36	rc = GetLastError();
37	FreeLibrary(hInst);
38	printf("\n\terror %d\n",rc);
39	}
40	
41	QRCodeINV("AA12345678", "1001231", "150000", "1234", 1000000, 100, 100,
42	"12345678", "87654321", "12344321", "43211234",
43	"05D4A324ABAF4A570E64E572221E438B", out, errorCode);
44	printf("ErrorCode:%d\n",*errorCode);
45	printf("%s", out);
46	
47	}else
48	{
49	printf("\n\tload Library fail\n");
50	}
51	free(array);
52	free(errorCode);
53	return 0;

54	}
55	
56	
57	
58	

五、QR Code 線上解密驗證

營業人可透過登入電子發票整合服務平台來進行線上解密驗證，可透過輸入密碼種子或加密金鑰來進行 QR Code 的解密驗證，以確認此 QR Code 之可用與完整性，操作流程如下：

1. 以管理員身份登入平台並點選下圖「QRCode 解密驗證」功能



2. 使用者可選擇以密碼種子或 AES 金鑰進行 QRCode 解密驗證

現在位置 / [人員帳號與權限管理](#) > [密碼及種子管理](#) > QRCode解密驗證

輸入欲解密之QRCode字串

QRCode加密字串	AA1234567810412191234000000b4000000b40000000054185095dSypnr83S3oOPU5HiEx49v/==
QRCode解密方式	<input checked="" type="radio"/> 密碼種子 <input type="radio"/> 32碼金鑰(16進制)
QRCode密碼種子	12345678

※QRCode解密之密碼種子與您加密時所使用之密碼種子相同

 解密驗證

QRCode密碼種子:12345678
QRCode加密字串:
AA1234567810412191234000000b4000000b40000000054185095dSypnr83S3oOPU5HiEx49w=
=

現在位置 / [人員帳號與權限管理](#) > [密碼及種子管理](#) > QRCode解密驗證

輸入欲解密之QRCode字串

QRCode加密字串	AA1234567810412191234000000b4000000b40000000054185095dSypnr83S3oOPU5HiEx49v/==
QRCode解密方式	<input type="radio"/> 密碼種子 <input checked="" type="radio"/> 32碼金鑰(16進制)
金鑰	6647A889B4B5912BECB5D01065CCD670

※QRCode解密之金鑰與您加密時所使用之金鑰相同

 解密驗證

AES金鑰: 6647A889B4B5912BECB5D01065CCD670
QRCode加密字串:
AA1234567810412191234000000b4000000b40000000054185095dSypnr83S3oOPU5HiEx49w==

3. 驗證成功時，會出現解密資訊

解密結果		
發票資訊		明文
發票字軌：	AA12345678	AA12345678
發票開立日期：	1041219	
隨機碼：	1234	1234
銷售額：	180.0	
總額：	180.0	驗證成功
買受人統編：	00000000	
營業人統編：	54185095	
密文：	dSypnr83S3oOPU5HiEx49w==	

1. 紅色框框上面的欄位是發票號碼下面欄位是隨機碼，如果與電子發票證明聯一致表示驗證通過。

2. 請將上面的欄位與電子發票證明聯比對:發票號碼、開立日期、隨機碼、總額、營業人統編、買受人統編(有打統編)等。

3. 請與前一頁QRCode加密字串的最後面24位與密文比對是否一致。

4. 如驗證失敗時，畫面右上方會出現彈跳視窗，顯示驗證錯誤

解密結果		
發票資訊		明文
發票字軌：	AA12345678	驗證錯誤
發票開立日期：	1041219	
隨機碼：	1234	驗證錯誤
銷售額：	180.0	
總額：	180.0	驗證失敗
買受人統編：	00000000	
營業人統編：	54185095	
密文：	dSypn	

紅色框框上面的欄位是驗證錯誤非發票號碼下面欄位是驗證錯誤非隨機碼，表示驗證失敗其他都不要再檢查

參、發票機敏欄位加密

營業人在使用 Turnkey 進行發票資料上傳前，需確認發票檔案內容是否有使用到機敏欄位填寫消費者個人資料，例如信用卡號、金融卡號等資訊，如有的話，需使用電子發票整合服務平台所提供之加密程式進行加密作業後再進行資料上傳。目前提供 Windows 環境下 .Net 版本 API 可供使用，說明如下：

一、API 使用說明

當營業人使用電子發票整合服務平台所提供之 API 時，須先使用[產生加密金鑰]工具(請參考第伍章)來產生加密金鑰。金鑰將以Hex(16進制)呈現，使用將此字串(AESKey)和發票欲加密字串(plainText)當作輸入參數帶入API中，即可得到加密後字串。

二、API 介面說明

API 介面如下：

英文名稱	中文名稱	類別	欄位必要性
plainText	欲加密字串	字串	M
AESKey	加密所使用之金鑰	字串	M

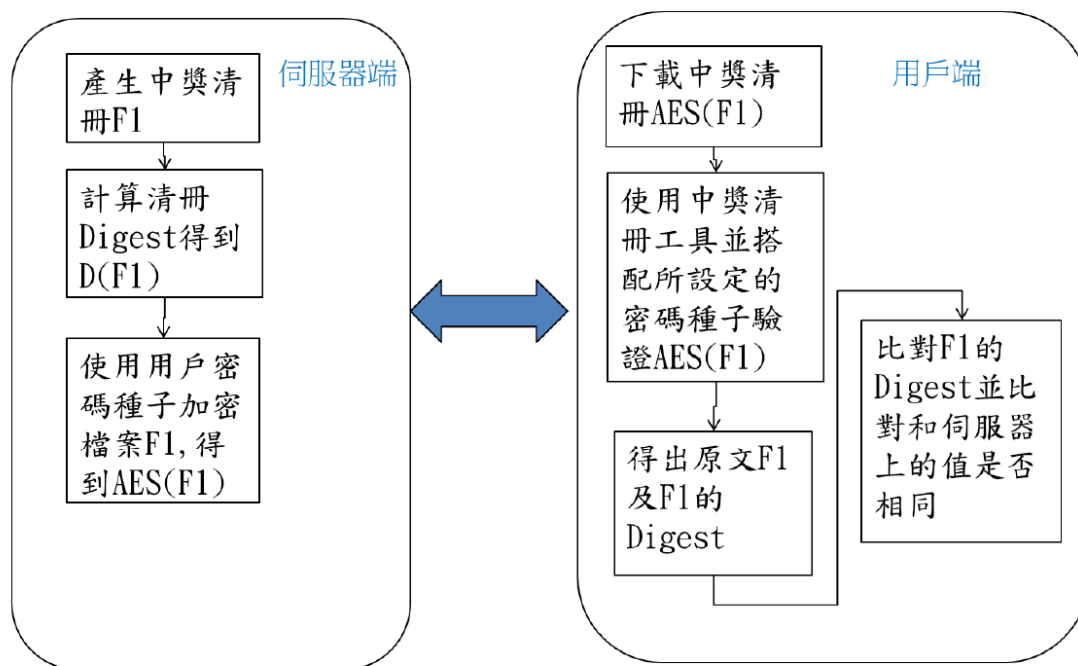
三、API 範例(.NET)

加解密程式範例如下，完整範例可以參考壓縮檔中 sample/net/StrEnc_Sample.cs

24	using System;
25	using System.Collections.Generic;
26	using System.Linq;
27	using System.Text;
28	
29	namespace SampleProject
30	{

31	class Sample
32	{
33	static void Main(string[] args)
34	{
35	com.tradevan.qrutil.QREncrypter qrEncrypter = new
36	com.tradevan.qrutil.QREncrypter();
37	try
38	{
39	String result = qrEncrypter.AESEncrypt("Test",
40	"78D92C1FA999954120227B664B29FF93");
41	
42	}
43	catch (Exception e)
44	{
45	Console.WriteLine(e.Message);
46	}
	Console.ReadLine();
	}
	}

肆、下載中獎清冊



此章節主要描述用戶下載中獎清冊作業流程及相關工具說明，如上圖所示，此機制主要架構在前述第一章中[連線電子發票整合服務平台點選密碼及種子管理(下載清冊) 設定加密密碼]的作業，即用戶須要先到電子發票整合服務平台上設定中獎清冊所使用的密碼種子，並搭配電子發票所提供之用戶端工具來達到清冊解密及驗證完整性的作業。接來來章節描述工具使用方式，相關工具皆放在在壓縮檔中 tool 目錄下。工具須使用 Sun JDK1(1.6)以上版本來執行。

工具執行方式分為 Command Mode 及 UI Mode 兩種。建議直接使用 UI Mode 來執行。

一、UI Mode 執行方式

(一) 加密檔案及計算 Digest(EncryptUI.bat)

1. 說明

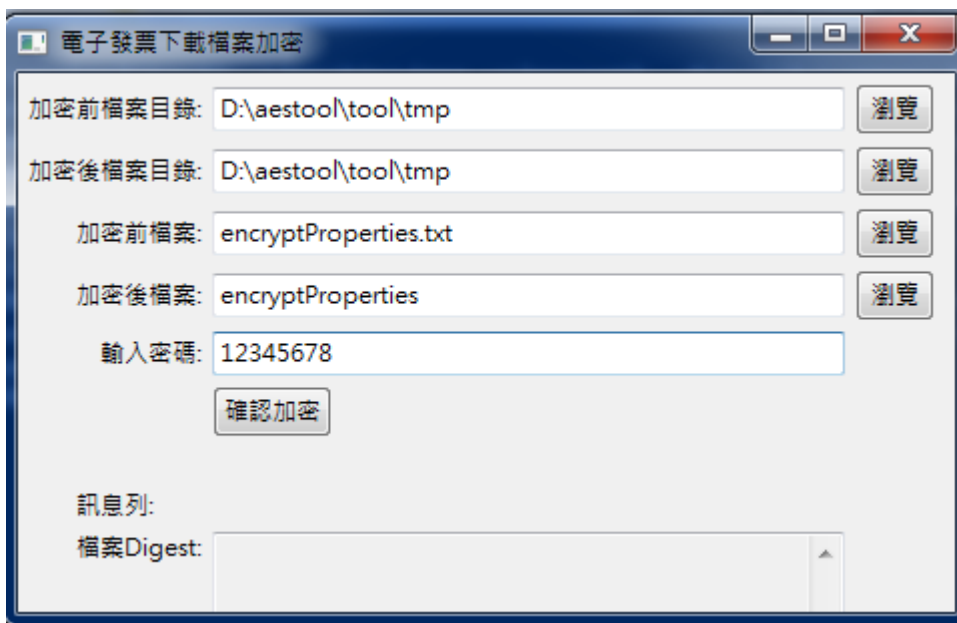
此UI主要以檔案為單位做加密的動作。

2. 執行步驟

執行 EncryptUI。輸入項目如下：

1. 欲加密檔案路徑，點選瀏覽選取。-Ex: D:\aestool\tool\tmp
 2. 加密完成檔案路徑，點選瀏覽選取。-Ex: D:\aestool\tool\tmp
 3. 欲加密檔案，點選瀏覽選取。-Ex: encryptProperties.txt
 4. 加密完成檔案，預設為欲加/解密檔案名，點選瀏覽選取。
-Ex: encryptProperties
 5. 輸入密碼種子。-Ex: 12345678
 6. 點選確認加密，開始編碼。
- 訊息會顯示於訊息列。

Digest 會寫顯示於檔案 Digest，可複製不可修改。



電子發票下載檔案加密

加密前檔案目錄: D:\aestool\tool\tmp 瀏覽

加密後檔案目錄: D:\aestool\tool\tmp 瀏覽

加密前檔案: encryptProperties.txt 瀏覽

加密後檔案: encryptProperties 瀏覽

輸入密碼: 12345678

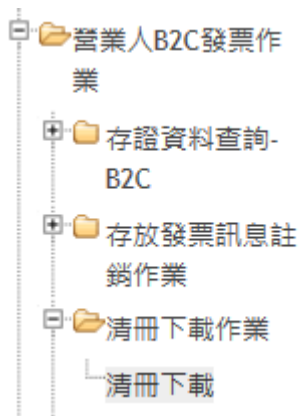
確認加密

訊息列: C000 已完成編碼

檔案Digest: C48C2721F557500CCE36198A126DCEADF3CF414
A

(二) 解密檔案及計算 Digest(DecryptUI.bat)

1. 首先至電子發票整合服務平台下載中獎清冊，下面功能選單點選清冊下載



2. 輸入電子發票中獎清冊的年期別，執行查詢功能鍵


清冊下載

* 清冊年月 104 年 9-10月

查詢

3. 點選下載電子發票中獎清冊

清冊下載					
序號	清冊年月	清冊名稱	檔案名稱	產生日期時間	檔案下載
1	104年9-10月	會員中獎清冊	Z_23060248_10410_20151127162139.bin	2015-11-28	下載

 10 1/1

4. DecryptUI.bat 說明

DecryptUI.bat此UI主要以檔案為電子發票中獎清冊解密的動作。

4-1. 執行步驟

執行DecryptUI。輸入項目如下：

4-1-1. 欲解密檔案路徑，點選瀏覽選取。-Ex:

D:\aestool\tool\tmp

4-1-1. 解密完成檔案路徑，點選瀏覽選取。

-Ex:D:\aestool\tool\tmp

4-1-3. 欲解密檔案，點選瀏覽選取。-Ex:

encryptProperties.bin

4-1-4. 解密完成檔案，預設為欲解密檔案名，點選瀏覽選取。

-Ex: encryptProperties

4-1-5. 輸入密碼種子。-Ex:12345678

(1)若之前有設定過密碼種子者，請輸入密碼種子之密碼。

(2)若未設定過密碼種子者，請以下列方式輸入密碼：

統編前四碼+期別+統編後四碼。

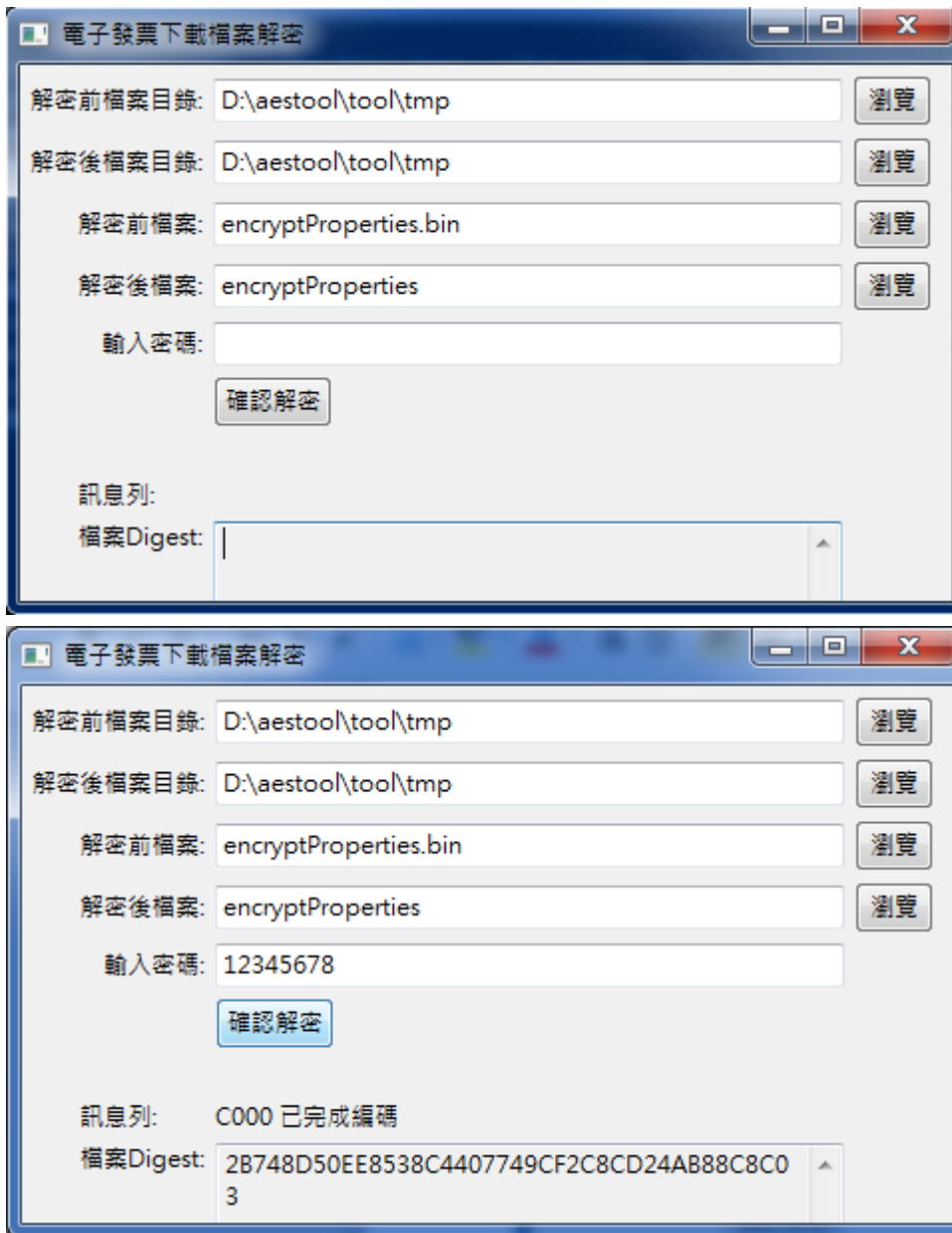
EX：此次期別為-20160102，若統編為 12345678

密碼則為 1234201601025678

4-1-6. 點選確認解密，開始解碼。

訊息會顯示於訊息列。

Digest會寫顯示於檔案Digest，可複製不可修改。



二、Command Mode 執行方式

(一) 加解密檔案 (decrypFile.bat/decrypFile.sh)

1. 說明

此工具主要針對以檔案為單位做加解密的動作。

2. 執行步驟

執行decryptFile來做檔案的加密解密。輸入項目如下：

1. 要執行的運算(加密或解密)-ex:1
2. 輸入密碼種子-ex:changit
3. 輸入來源檔案-ex: D:\Tmp\abc.txt
4. 輸入輸出檔案-ex:D:\Tmp\abc.txt.enc

```
===Enter [q] to exit program===
Enter 1:encrypt or 2:decrypt: 1
Enter passphrase: changit
Enter Source File Path: D:\Tmp\abc.txt
Enter Target File Path: D:\Tmp\abc.txt.enc
[2011/11/24 16:57:41][INFO][][ ] - begin gen key...
[2011/11/24 16:57:41][INFO][][ ] - end gen key...(OK)
[2011/11/24 16:57:41][INFO][][ ] - com.tradevan.geinv.kms.dist.DistKMSService be
gin init...
[2011/11/24 16:57:41][INFO][][ ] - com.tradevan.geinv.kms.dist.DistKMSService be
gin init...(OK)
[2011/11/24 16:57:41][INFO][][ ] - get encrypt cipher...
[2011/11/24 16:57:41][INFO][][ ] - com.tradevan.geinv.kms.dist.DistKMSService be
gin init Encrypt cipher...
[2011/11/24 16:57:42][INFO][][ ] - com.tradevan.geinv.kms.dist.DistKMSService be
gin init Encrypt cipher...(OK)
[2011/11/24 16:57:42][INFO][][ ] - get encrypt cipher...OK
[2011/11/24 16:57:42][INFO][][ ] - encrypt file(D:\Tmp\abc.txt) to file(D:\Tmp\abc
.txt.enc)...
[2011/11/24 16:57:42][INFO][][ ] - encrypt file(D:\Tmp\abc.txt) to file(D:\Tmp\abc
.txt.enc)...OK
Result==>Success!
```

最後會顯示是否成功的訊息。若想結束程式只要輸入”q”，即可。

(二) 計算檔案 Digest (digestFile.bat/digestFile.sh)

1. 說明

此工具主要針對檔案做Digest運算，並將結果以Hex方式顯示。

2. 執行步驟

執行digestFile來做計算檔案Digest。輸入項目如下：

1. 輸入來源檔案-ex: D:\Tmp\abc.txt

```
===Enter [q] to exit program===  
Enter Source File Path: D:\Tmp\abc.txt  
Result(Hex)=>8F0AA2D5A7D2599C5353B0D0064A9C2EA6A53634
```

最後會顯示計算結果(以十六進位HEX顯示)。若想結束程式只要輸入” q” ，即可。

伍、 其他相關工具

相關工具皆放在在壓縮檔中 tool 目錄下。工具須使用 Sun JDK1(1.6)以上版本來執行。

一、 產生加密金鑰 (genKey.bat/genKey.sh)

(一) 說明

此工具搭配輸入使用者的 Passphrase，可產生出加密金鑰，並將結果以 Hex 方式顯示。

(二) 執行步驟

執行 digestFile 來做計

執行 genKey 來產生加密金鑰。輸入項目如下：

1. 輸入密碼種子-ex:changit

```
---Enter [q] to exit program---  
Enter passphrase: changit  
[2011/11/24 17:16:02][INFO][][ ] - begin gen key...  
[2011/11/24 17:16:03][INFO][][ ] - end gen key...<OK>  
[2011/11/24 17:16:03][INFO][][ ] - com.tradevan.geinv.kms.dist.DistKMSService be  
gin init...  
[2011/11/24 17:16:03][INFO][][ ] - com.tradevan.geinv.kms.dist.DistKMSService be  
gin init...<OK>  
Result(Hex)==>7DE1747AA8613314C0C95ACCC5568911
```

最後會顯示計算結果(以十六進位 HEX 顯示)。若想結束程式只要輸入” q” ，即可。