

捷而思股份有限公司

智慧手持裝置的行動安全應用

智慧**行動政府**· 打造掌上生活

i-Taiwan 無線上網服務

熱點查詢

APP應用

資訊加值

推文至：[f](#) [P](#) [t](#)





公司簡介

- 1 身份認證及資料加解密、安全訊息傳輸的專業廠商
- 2 公司成員從事資安研發之平均年資超過10年
- 3 電子化政府行動資安解決方案研發先驅廠商
- 4 產品符合國際標準及規範，立足臺灣積極拓展海外拓銷
- 5 已申請臺灣五項專利、中國兩項及美國一項專利

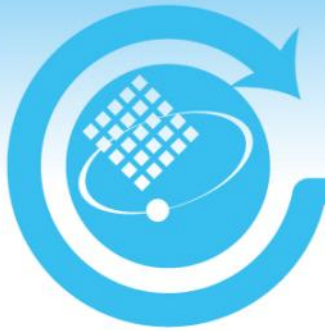




Award

◆ 2013年11月獲得亞太資通訊奧斯卡獎 APICTA Award 隱私及資安產品組的





捷而思資安專業團隊



豐富經驗

- 成員豐富大型專案規劃經驗
- 具資訊系統架構規劃經驗及能力

- ◆ 主要從事資訊安全產品研發，資訊安全專案承接以及顧問服務。
- ◆ 客戶物件除國內政府、銀行及企業外，也積極從事海外拓銷，合作夥伴超過三十多個國家。

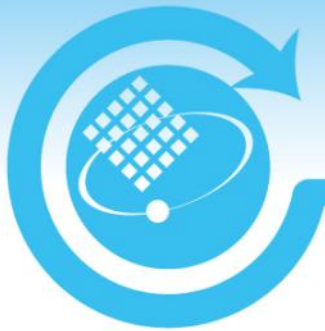
www.jrsys.com.tw

128個國家地區來訪



- ◆ 相關經驗
 - 外交部單一登入及行動公務
 - 移民署生物識別規劃案
 - 食品管理局多重訊息平臺
 - 華義國際單一簽入系統
 - 中央氣象局憑證建置案
 - 北京四通智慧行動憑證建置
 - 國合會中美洲電子化政府顧問
 - hTC CCC行動憑證系統導入
 - 土地銀行金融憑證應用
 - 大昌證券網路下單憑證應用

jrsys



jrsys技術能量



Core Framework

Core Library
(Dynamically loaded library/Java Class)

ActiveX Component
(COM)

FireFox Google-Chrome
(Plug-in/Add-on)

APP Core Framework
(iOS/Android)

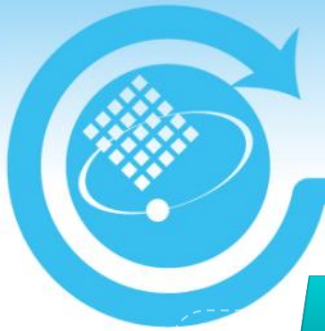
jrsys Secure Foundational SDK (Support for C/C++ and Java)

Cryptographic Message Syntax Standard

Cryptographic Algorithm

ASN.1
(Abstract Syntax Notation One)

Mathematic
Big-Integer



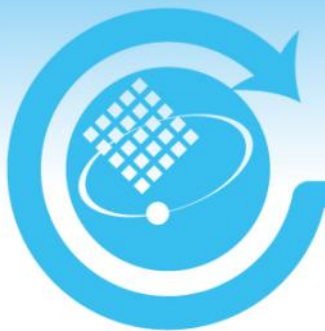
行動化時代來臨

過去在PC時代，智慧卡或是token等PKI方案，可達到雙因素認證的效果，避免帳號密碼遭竊，確保身分認證的安全。

行動化時代來臨，雙因素認證也必不可失，面對眾多類型行動裝置(ex. iOS、Android、WP8)等，使用者需要符合相對應的方案，才能避免駭客的侵擾。

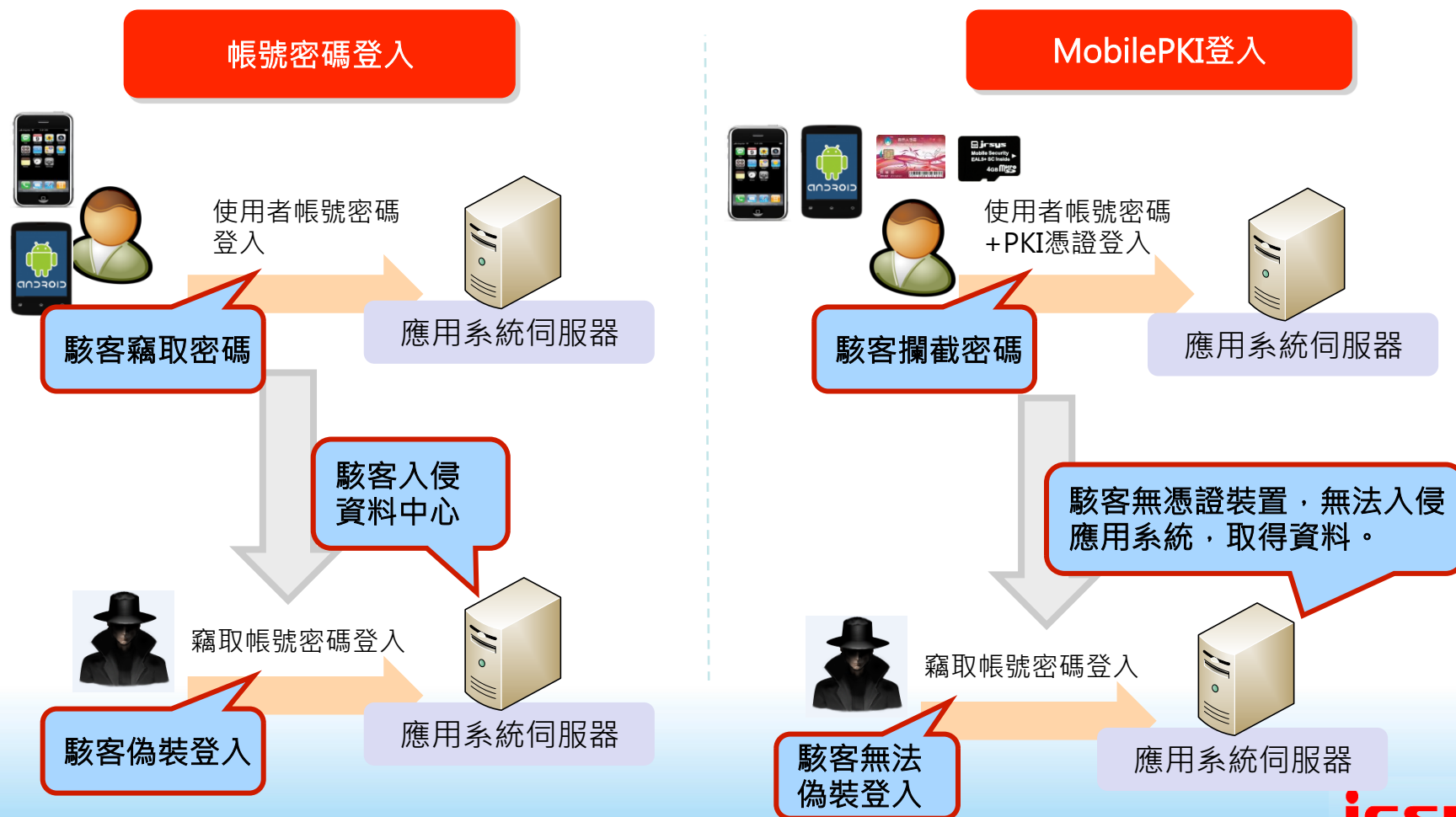
為講求效率，期望能在安全的環境情況下，能夠隨時隨地的處理公事。不同於一般的電腦環境，行動裝置必須面對多元的環境。

將公務處理的流程導入行動化，需要符合行動裝置的簽核工具。使用者不需要攜帶筆記本就可以完成公事處。



安全的雙因素認證存取

- 帳號密碼易遭竊，只有帳號密碼登入的系統，容易被駭客入侵
- 雙因素認證的系統，駭客無實體安全智慧裝置，無法入侵系統



行動安全裝置

- Secure MicroSD
- Mobile Token
- 藍芽讀卡機



電腦 USB

Android迷你USB



PC/Android兩用USB碟

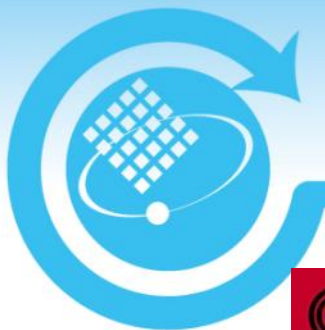
電腦 USB

蘋果接頭



PC/iOS兩用記憶碟





多用途安全MicroSD



CC EAL 5+
PBOC/QPBOC



安全的行動應用

行動安全 PDF

行動安全 e-Mail

手機信用卡
手機錢包
手機收銀機

行動認證/簽核

OTP一次性
動態密碼

數位簽章/加解密

JavaCard作業系統

SecureElement硬體安全晶片

產生不可匯出、
不能被複製的金鑰

RSA公私密金鑰
1024、2048

對稱函數
DES/3DES

通過EMV
信用卡組織認證

通過國際
CC EAL 5+認證

內建NFC天線

CC EAL5+
EMV/NFC
安全晶片

智慧手機MobilePKI電子
行動簽核、行動電子公務
應用的最佳選擇

安全行動載具



Secure MicroSD



CC EAL 5+
PBOC/QPBOC

iOS行動裝置

蘋果接頭

電腦
USB



全世界第一支蘋果/電腦雙用安全隨身碟

MobileToken有兩個接頭，一端連接iOS裝置，另一端USB連結PC端。

Android行動裝置

Android
Micro USB

電腦
USB



全世界第一支Android/電腦雙用安全記憶碟

MobileToken一端連接MicroUSB的Android裝置，另一端USB連結PC端。



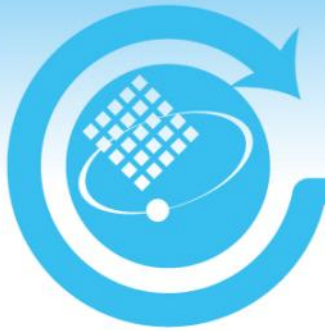
藍芽讀卡機



藍芽讀卡機

#	符合裝置
1	1. iOS 2. (iPhone、iPad)
2	1. 安卓 2. (Phone、Pad)
3	1. 桌上型電腦 2. 筆記本





藍芽讀卡機-iOS



The screenshots illustrate the following steps:

- Step 1:** The app interface shows a '連接藍芽讀卡機' (Connect Bluetooth Card Reader) button and a 'Load html file' button. The address bar contains 'http://192.168.232.105/i...'. The status bar shows '中華電信' (China Mobile), '上午9:41', and 46% battery.
- Step 2:** A dialog box prompts the user to '請輸入自然人憑證PIN碼...' (Please enter the Natural Person Digital Certificate PIN code...). Below the prompt is a text input field and two buttons: '取消' (Cancel) and '確定' (Confirm). The status bar shows '下午12:18' and 54% battery.
- Step 3:** A standard iOS keyboard is displayed over the app interface.
- Step 4:** The app displays a list of certificate details under the heading 'PKI 範例' (PKI Example). The details include: 憑證發行者 (Certificate Issuer), 憑證主旨 (Certificate Subject), 憑證啟始日期 (Certificate Start Date), 憑證到期日 (Certificate Expiry Date), 電子郵件 (Email), 身分證末四碼 (Last four digits of ID card), and Unique ID. A '重新整理' (Refresh) button is visible in the top right.
- Step 5:** The app shows a '智慧卡登入' (Smart Card Login) screen with a '簽章憑證匯出' (Export Signature Certificate) button. A loading indicator and the text '操作中，請勿將卡片退出...' (Processing, please do not remove the card...) are shown. The status bar shows '下午12:18' and 54% battery.



蘋果/電腦雙用安全隨身碟

PKI 範例

智慧卡

- 登入
- 登出
- 電子簽章 (RSA PKCS#7)
- 執行簽章
- 簽章成功後，取得簽章值
- 驗證簽章值
- X.509 憑證

匯出簽章憑證

解譯 X.509 憑證

憑證序號

憑證發行者

憑證主旨

憑證啟始日期

憑證到期日

電子郵件

身分證末四碼

Unique ID

Jrsys Internal

Jrsys International Corp.

請輸入智慧卡 PIN 碼...
捷而思 Demo 版本 (1.0.9 Demo)

取消 確定

簽章

簽於 computex

主旨：申請各單位新進同仁電腦設備

說明：本(系所單位)因新進同仁需要電腦設備，擬採購 Apple MacBook Pro 設備金額約需 50000 元。依中央機關未達公告金額採購招標辦法第二條第一項第一款規定擬採限制性招標方式辦理採購，請請核示。

擬辦：
一、申請一套電腦設備予新進同仁使用。
二、申請項目中申請數量多於一項的零組件，作為升級和儲存設備之用途。

敬請
總經理 XXX

憑證資訊

57D457093AF796E9

CN = JrsysCA

emailAddress = computex@jrsys.com.tw, CN = computex, C = TW

Tue May 28 09:34:22 2013

Fri Jun 28 09:34:22 2013

提交簽章

Jrsys International Corp.

選擇 Jrsys Mobile PKI 範例...

- I-Key PKI Demo
- Document Signing Demo
- Default Local Page
- 基本智慧卡功能操作
- 文件簽核範例
- 預設本機範例頁面





捷而思行動安控元件



OTP 動態密碼
Digital Signature 行動認證
En/Decrypt 行動資料加密
Cloud Login 雲端安全認證

Jrsys Mobile Security Suite



iOS SDK



Android SDK

搭配各種安全的行動載具



軟體憑證



電腦/安卓兩用USB
接觸及非接觸讀卡機



藍芽讀卡機



加密晶片
MicroSD



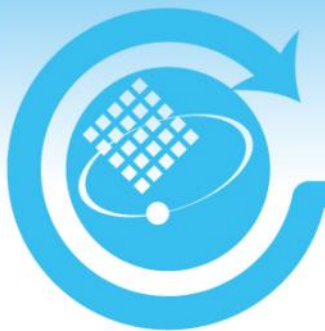
PC/Android
雙向USB
Token



PC/iOS Dual
Adaptor



行動簽核解決方案 Mobile Signing Solution



行動簽核架構-APP Signing

- MobileHIS系統提供 APP。
- 提供簽核的WEB框架，讓各APP套用。
- 不需要臨時憑證架構，自然人憑證，醫事人員卡均可適用。
- 畫面以及操作介面人性化。

jrsys 行動簽核元件

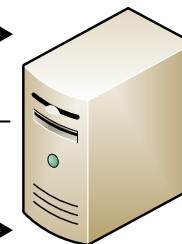
● 元件發出簽合需求，以及簽核資訊。

● 使用者登入 HIS APP

● 應用系統要求使用者簽核

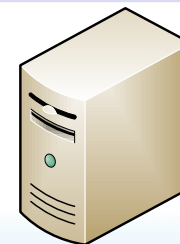
● 回傳簽章資料

● 使用者輸入Pin 簽章。



HIS平台
NIS平台

● 驗證簽章資料是否正確。



行動電子憑證驗證平臺

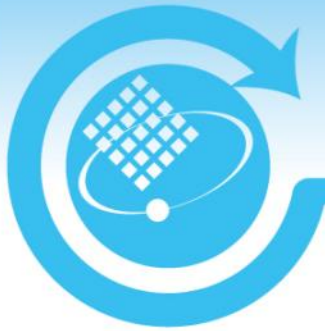




行動電子憑證驗證平臺

- ◆ 目的: 達到系統使用憑證驗證管理。
- ◆ 應用範圍:

- 1 企業內部系統，為達到憑證登入管控
- 2 企業電子公文或流程資料需要標準簽名程式
- 3 企業供應鏈系統，可應用工商憑證達到資料確認
- 4 需要驗證多種憑證，可以統一管理驗證憑證
- 5 政府單位資料交換，需要標準簽名格式
- 6 金融單位需要驗證標準金融憑證格式



行動電子憑證驗證平臺

◆ 系統特色:

- 支持國內外各種憑證的驗證功能。
- 可設定控管系統管理員登入系統許可權之安全機制。
- 可驗證交易時產生的數位簽章，遵循PKCS#7與W3C XMLSignature等國際標準規格。
- 支援CRL或OCSP驗證等級、支援CRL週期設定排程、手動或自動下載機制。
- 提供Web-based管理介面，提供使用者的憑證資料管理、系統管理及憑證類別管理等功能。
- 提供完整之登入稽核記錄及事件通知功能，其事件與紀錄內容需包含何人、何地(Client IP)、何時、及做何事等資訊，其憑證使用者登入需記錄其登入數位簽章資料，以供驗證。



功能畫面說明

◆ 信任憑證管理清單檢視

Jrsys 憑證驗證伺服器

Certificate validation authority

[Home](#) | [About Us](#) | [Products](#) | [Contact](#)

信任憑證管理

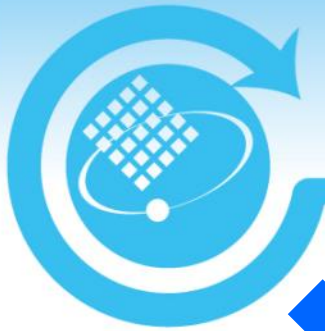
[新增信任憑證](#)

[樹狀檢視](#) | [清單檢視](#)

第一頁 **1** 最後一頁 共 1 頁, 前往第 頁 前往

id	別名	有效日起迄	主旨	自簽憑證	是否廢止?	功能
36	GCA2	2003-03-03 00:00:00.0至2023-03-03 00:00:00.0	OU=政府憑證管理中心, O=行政院, C=TW	false	0	設定 檢視CRL 刪除
38	uIAM	2009-05-15 00:00:00.0至2039-05-15 00:00:00.0	CN=uIAM, DC=rd2, DC=ares, DC=com, DC=tw	true	0	設定 檢視CRL 刪除
41	HCA	2008-08-18 00:00:00.0至2028-08-18 00:00:00.0	OU=醫事憑證管理中心, O=行政院, C=TW	false	0	設定 檢視CRL 刪除

© 2010 JRSYS INTERNATIONAL CORP. All rights reserved.
- JRSYS VA - 2011/03/04 updated



信任憑證管理

◆ 新增憑證畫面

Jrsys 憑證驗證伺服器

Certificate validation authority

[Home](#) | [About Us](#) | [Products](#) | [Contact](#)

管理

- 信任憑證管理
- 憑證驗證服務
- 黑名單服務
- CMS服務
- OCSP服務
- 排程查詢
- 角色管理
- 使用者管理
- 修改密碼
- 登出

服務

登入狀態

信任憑證管理

憑證下載 | **憑證明細**

別名:	GCA
憑證序號:	339939084106886165023589893722676428373
主質:	OU=政府憑證管理中心, O=行政院, C=TW
發行者:	O=Government Root Certification Authority, C=TW
有效日期起:	2003-03-03
有效日期迄:	2023-03-03
憑證鏈:	O=Government Root Certification Authority, C=TW OU=政府憑證管理中心, O=行政院, C=TW
CRL網址:	<input type="text"/>
CRL更新方式:	<input checked="" type="radio"/> 手動更新 <input type="radio"/> 每日 <input type="radio"/> 每周
更新時間:	<input type="text"/>
每周更新時間:	星期日
CARL檢查:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
OCSP網址:	<input type="text"/>
OCSP憑證:	<input type="text"/> <input type="button" value="瀏覽..."/>
<input checked="" type="checkbox"/> 是否驗證OCSP回應?	

© 2010 JRSYS INTERNATIONAL CORP. All rights reserved.
- JRSYS VA - 2011/03/04 updated



黑名單(憑證廢止清單)服務畫面

Jrsys 憑證驗證伺服器

Certificate validation authority

[Home](#) | [About Us](#) | [Products](#) | [Contact](#)

管理

- 信任憑證管理
- 憑證驗證服務
- 黑名單服務
- CMS服務
- OCSP服務
- 排程查詢
- 角色管理
- 使用者管理
- 修改密碼
- 登出

服務

登入狀態

黑名單服務

檢驗憑證

第一頁 **1** 最後一頁 共 1 頁,前往第 頁 前往

crId	certId	別名	subjectDN	此次更新時間	下次更新時間	CRLEntry 數量	功能
15	36	GCA2	OU=政府憑證管理中心, O=行政院, C=TW	2011-03-04 09:49:38.234	2011-04-04 00:00:00.0	1281	檢視CRL 立即更新CRL
17	38	uIAM	CN=uIAM, DC=rd2, DC=ares, DC=com, DC=tw	2011-03-02 11:03:43.314	2011-03-09 10:30:43.0	34	檢視CRL 立即更新CRL
20	41	HCA	OU=醫事憑證管理中心, O=行政院, C=TW	2011-03-04 09:51:58.804	2011-04-01 23:59:59.0	8313	檢視CRL 立即更新CRL

© 2010 JRSYS INTERNATIONAL CORP. All rights reserved.
- JRSYS VA - 2011/03/04 updated



憑證廢止清單明細檢視

Jrsys 憑證驗證伺服器

Certificate validation authority

[Home](#) | [About Us](#) | [Products](#) | [Contact](#)

管理

- 信任憑證管理
- 憑證驗證服務
- 黑名單服務
- CMS服務
- OCSF服務
- 排程查詢
- 角色管理
- 使用者管理
- 修改密碼
- 登出

服務

登入狀態

信任憑證管理

Certificate alias	GCA2
issuer:	OU=政府憑證管理中心, O=行政院, C=TW
CRL url:	http://gca.nat.gov.tw/repository/GCA4/CRL/complete.crl
CRL entries count:	1281

第一頁 **1** 2 3 4 5 6 7 8 9 10 下一頁 最後一頁 共 129頁,前往第 頁 前往

id	憑證序號	廢止時間	廢止理由
92346	100479574220071254462058034260150009173	2008-02-04 00:00:00.0	3
92213	100962358915989875115846048768177521214	2008-04-21 00:00:00.0	3
91528	101117915124951805303083398792441326995	2006-09-08 00:00:00.0	3
91860	101316523914328359775788699838835661870	2007-07-12 00:00:00.0	3
92418	101975182471381928661459793240376416263	2009-11-24 00:00:00.0	3
92667	102164940204760216873691451936572931082	2010-10-14 00:00:00.0	3
92359	102666284608505624764397570667862189389	2008-11-27 00:00:00.0	3
92381	102718516356566706727584813183805276521	2006-08-29 00:00:00.0	5
92487	10293889236908658820124575049745560125	2009-08-10 00:00:00.0	5
91760	10323390652008200330115036266232196104	2008-02-04 00:00:00.0	3

© 2010 JRSYS INTERNATIONAL CORP. All rights reserved.
- JRSYS VA - 2011/03/04 updated



憑證驗證服務

◆ 驗證結果呈現畫面

Jrsys 憑證驗證伺服器
Certificate validation authority

[Home](#) | [About Us](#) | [Products](#) | [Contact](#)

管理

- 信任憑證管理
- 憑證驗證服務
- 黑名單服務
- CMS服務
- OCSP服務
- 排程查詢
- 角色管理
- 使用者管理
- 修改密碼
- 登出

服務

登入狀態

憑證驗證服務

憑證從檔案:

憑證從Base64:

驗證方式:

輸出格式:

檢驗結果

憑證序號:	9836!	26809
主管:	SERIALNUMBER=00000000100, CN=, O=行政院, C=TW	
發行者:	OU=政府憑證管理中心, O=行政院, C=TW	
有效日期起:	2006-11-07	
有效日期迄:	2011-11-07	

檢驗結果

檢驗規則名稱	檢驗結果	檢驗訊息
Signature	true	Signature checked pass!
DateValidity	true	DateValidity checked pass!
CRL	true	CRL checked pass!
OCSP	true	OCSP checked pass!
CRLCheckOnline	false	CRLCheckOnline checked fail! Cause:CRL URL is empty.
HasDigitalSignatureKeyUsage	true	HasDigitalSignatureKeyUsage checked pass!
CAIsRevoked	true	CAIsRevoked checked pass!



OCSP憑證驗證服務

◆ 驗證結果呈現

Certificate validation authority

[Home](#) | [About Us](#) | [Products](#) | [Contact](#)

管理

- 信任憑證管理
- 憑證驗證服務
- 黑名單服務
- CMS服務
- OCSP服務
- 排程查詢
- 角色管理
- 使用者管理
- 修改密碼
- 登出

服務

登入狀態

OCSP服務

OCSP Service

發行者:

憑證序號1:

憑證序號2:

憑證序號3:

憑證序號4:

憑證序號5:

憑證序號6:

憑證序號7:

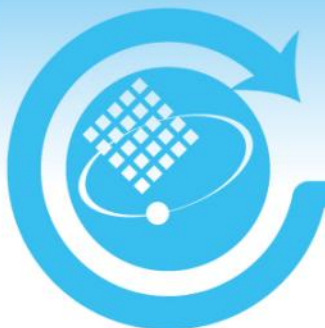
憑證序號8:

憑證序號9:

憑證序號10:

憑證序號	是否廢止?	廢止時間	廢止理由
98365395672900162679087993972943826809	否		
100479574220071254462058034260150009173	是	Mon Feb 04 15:00:18 CST 2008	3

© 2010 JRSYS INTERNATIONAL CORP. All rights reserved.
- JRSYS VA - 2011/03/04 updated



應用系統管理

應用程式系統管理

應用程式設定停用!

新增應用系統設定

第一頁 1 最後一頁 共 1 頁,共 3 條,前往第 頁 前往

id	應用系統名稱	來源IP	通行碼	狀態	功能
1	app-11111	192.168.232.45,127.0.0.1	1234567890	Enable	設定 停用 刪除
2	app2222	192.168.232.20,192.168.232.3	12345	Enable	設定 停用 刪除
3	Portal	192.168.123.123	1234567890	Disable	設定 啟用 刪除

應用程式系統管理

應用系統名稱:

來源IP:

通行碼:

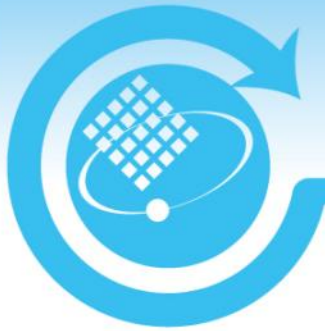
描述:

應用程式系統管理

新增應用系統設定

第一頁 1 最後一頁 共 1 頁,共 2 條,前往第 頁 前往

id	應用系統名稱	來源IP	通行碼	狀態	功能
1	app-11111	192.168.232.45,127.0.0.1	1234567890	Enable	設定 停用 刪除
2	app2222	192.168.232.20,192.168.232.3	12345	Enable	設定 停用 刪除



CMS憑證驗證服務

CMS驗證存證服務

驗證結果

驗證結果XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<pkcs7-signed-data-verify>
  <pkcs7-signed-data>
    <signer-infos>
      <signer-info>
        <certificate>
          <date-from>2006-11-07T11:20:03.000+08:00</date-from>
          <date-to>2011-11-07T11:20:03.000+08:00</date-to>
          <issuer>C=TW,O=行政院,OU=政府憑證管理中心</issuer>
          <issuer-der>3044310B300906035504061302545731123010060355040A0C09E8A18CE694
          <subject>C=TW,O=行政院,OU=研究發展考核委員會,CN=e管家,SERIALNUMBER=0000000010C
          <subject-der>3074310B300906035504061302545731123010060355040A0C09E8A18CE69
          <serial-number>4a007c712aca7e93654308e2fb2d2f79</serial-number>
          <key-usage>100000000</key-usage>
          <encoded>MIIElzCCAxegAwIBAgIQSgB8cSrKfpNIQwji+y0veTANBgkqhkiG9w0BAQUFADBEMQ
          <certificate-verify-rules>
            <verify-rule result="true" name="Signature"/>
            <verify-rule result="true" name="DateValidity"/>
            <verify-rule result="true" name="OCSP"/>
            <verify-rule result="true" name="HasDigitalSignatureKeyUsage"/>
            <verify-rule result="true" name="CAIsRevoked"/>
          </certificate-verify-rules>
          <certificate-verified>true</certificate-verified>
        </certificate>
        <signature-verified>true</signature-verified>
      </signer-info>
    </signer-infos>
  </pkcs7-signed-data>
  <verifyNo>201105060000003</verifyNo>
  <verified>true</verified>
  <status>0</status>
</pkcs7-signed-data-verify>
```



行動PKI安全應用解決方案



醫療行動應用





行動安全



動態密碼
每次不同
駭客無法
猜測密碼



電子郵件
簽名加密
解密之前
都是亂碼



全世界第一套Android Secure e-Mail
電子郵件硬體簽名加密解決方案
已與Outlook、Notes、Exchange整合

全世界第一套智慧行動可攜式電子檔PDF晶片簽名/加密系統



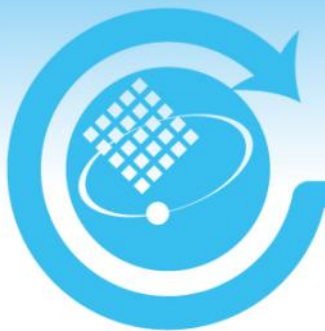
行動PDF簽名加密解決方案



全世界第一套Android SecurePDF可攜式電子檔晶片簽名/加密系統



手機接收加密之PDF緊急公文、報價單，輸入PIN碼解密、確認後立刻決行，安全快速又方便



可攜式安全電子檔



受文者：捷而思股份有限公司
發文日期：中華民國101年04月19日
發文字號：經商字第10102411500號
類別：普通件
密等及解密條件或保密期限：
附件：如文

主旨：為詳盡說明本部101
國際教育訓練活動

直接解密、批示及數位簽章



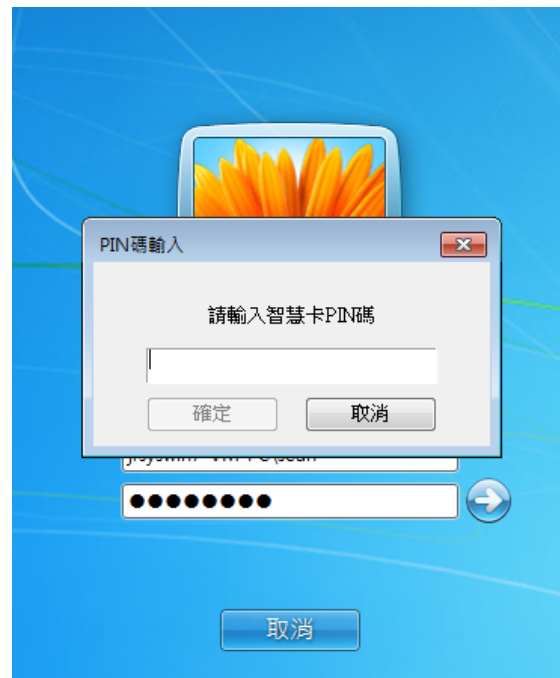
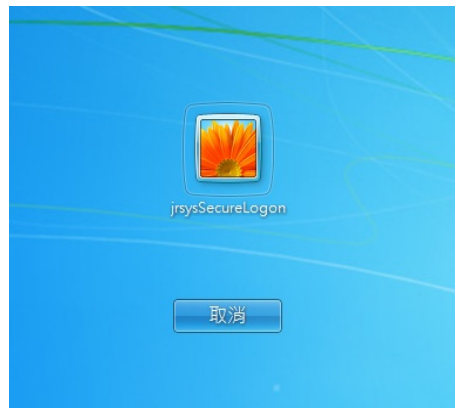


Windows安全憑證登入

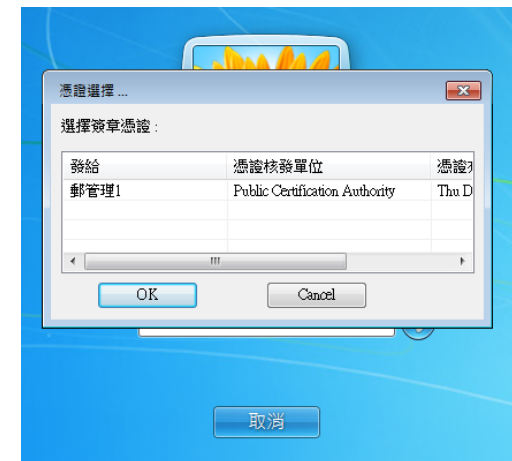
- Windows安全憑證登入解決方案
- 登入安全免煩惱，雙因數認證保障安全

Pin碼輸入保護

篩檢程式，只允許憑證登入

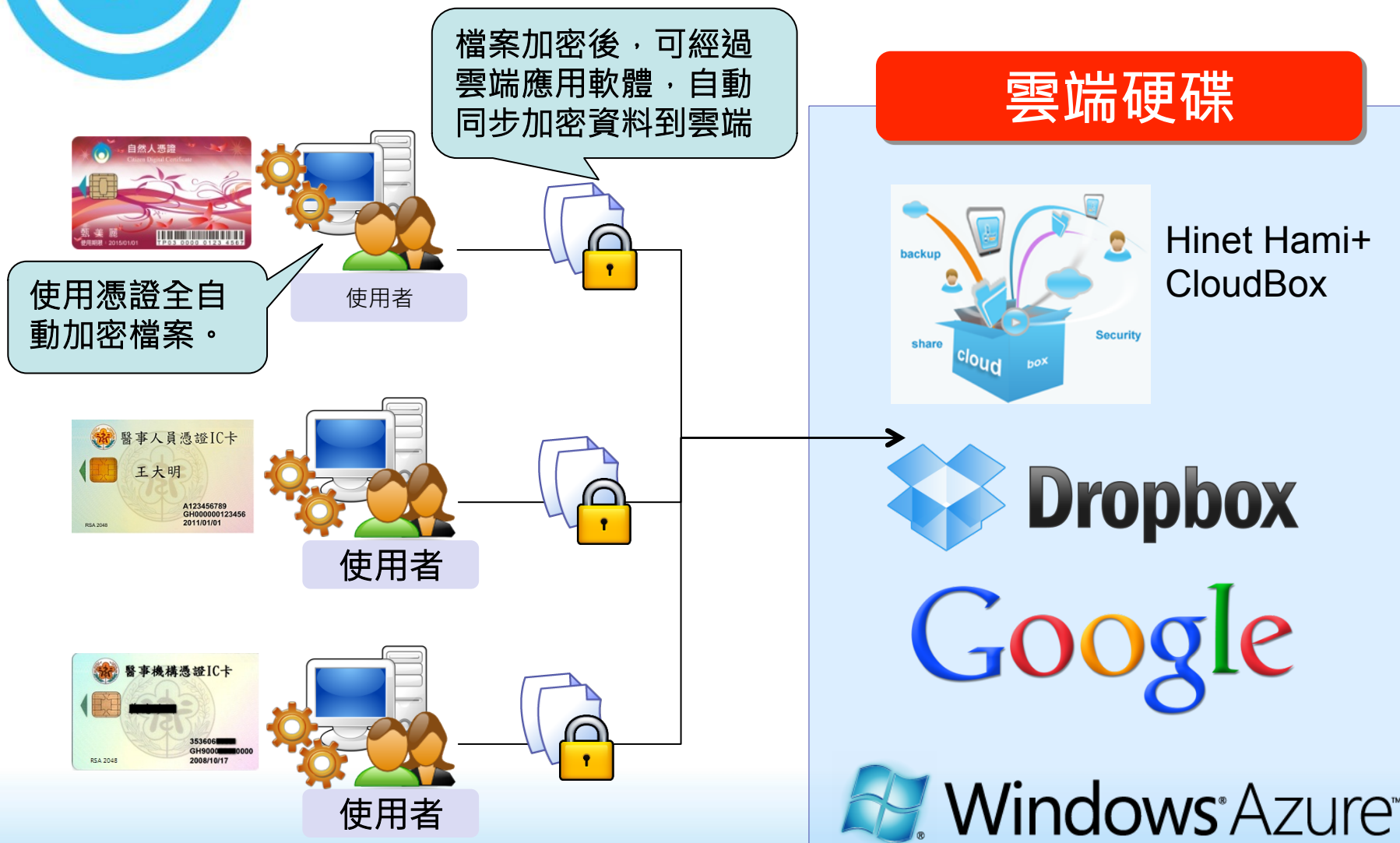


選擇卡片內的憑證



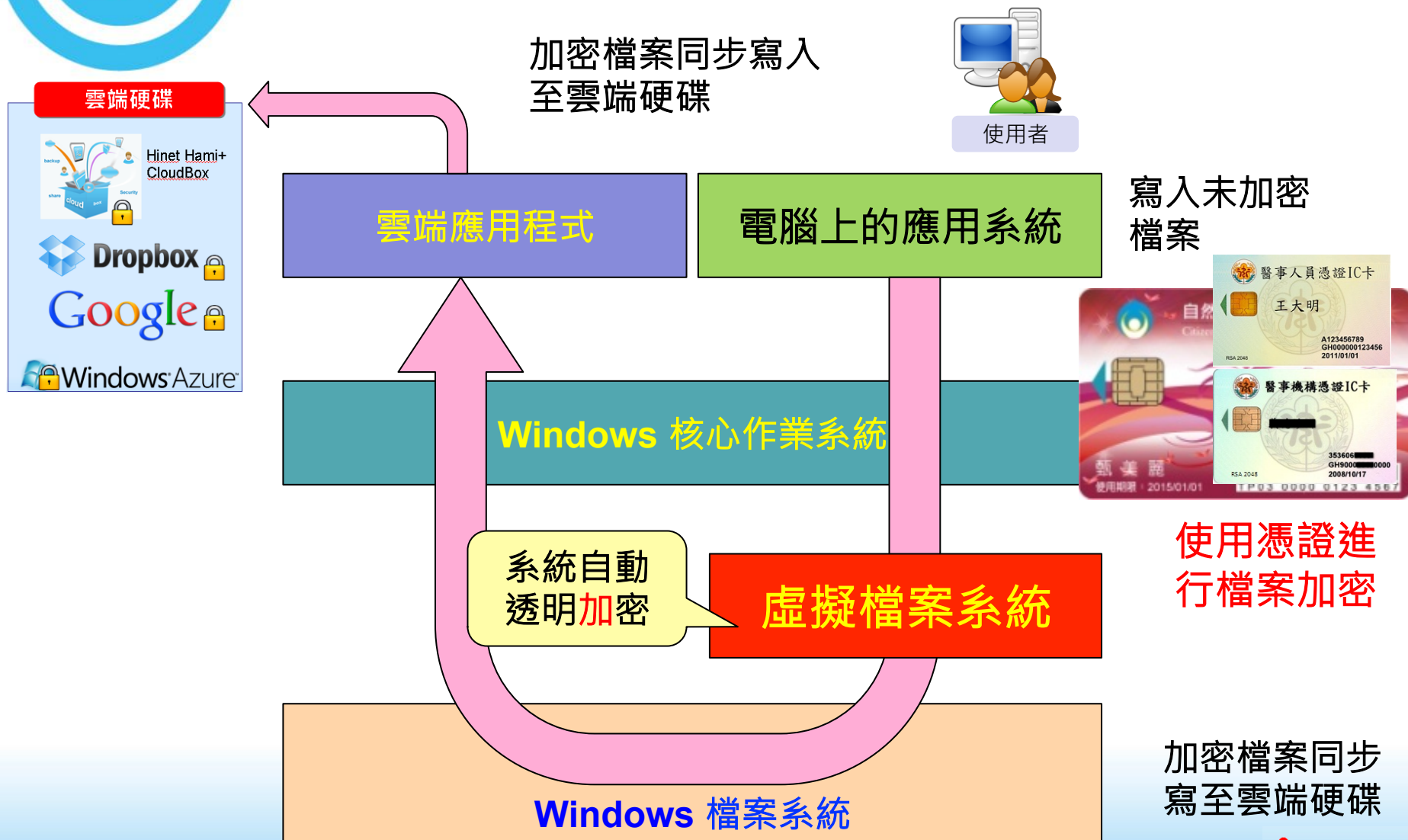


憑證安全雲儲存



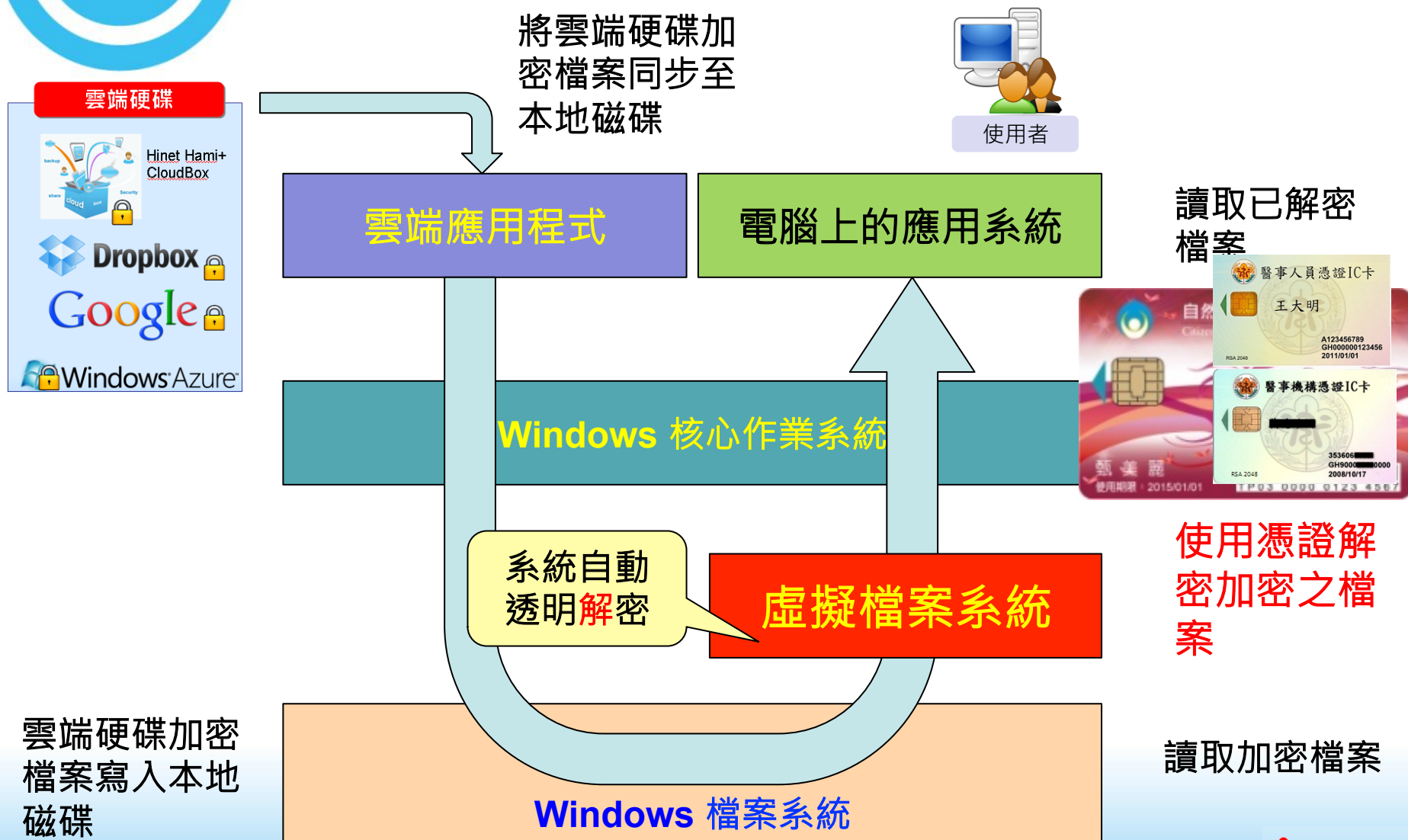


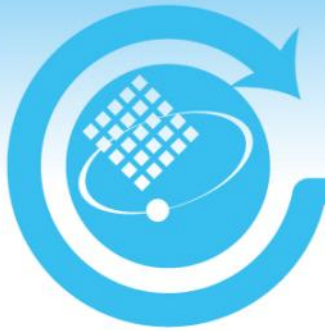
憑證安全雲儲存-儲存檔案





自然人憑證安全雲儲存-讀取檔案





憑證安全雲儲存

◆ 使用超方便

- 透過檔案總管，就可以自動透明加密檔案
- 不必修改微軟**Office**及各種應用系統，就可直接加密檔案
- 全民共爽最佳之安全雲儲存與備份解決方案

◆ 使用憑證

- 必須插入憑證，並輸入**PIN**碼才能解密檔案
- 使用憑證雙因子認證，完全不必擔心雲端硬碟之帳號密碼不小心外洩或被駭客入侵時，雲端檔案會被竊取

◆ 支援行動載具

- 透過藍芽讀卡機，手機也可以存取加密之雲儲存資料



捷而思 為您的智慧行動應用安全把關



URL: <http://www.jrsys.com.tw>

TEL: +886-2-2599-3797

本文件內容之文字、圖檔等相關資料，未經本公司書面同意，
不得轉載、複製或以任何方式提供予第三方使用