

{ 新世代 } 安全網絡人

CERTiZEN 教育手冊

甚麼是「公匙基礎建設」？

為安全網絡通訊而設的「數碼證書」

如何在信息進行加密及解密？



在社區更廣泛應用數碼證書及採用公匙基建科技
Wider Usage of Digital Certificate and Adoption of PKI Technology in the Community



給「新世代安全網絡人」

隨著社會的進步，電腦及互聯網的相繼出現與普及，網上溝通交流、商務交易、資料互換就愈趨普遍，網絡上的安全性、保密性、完整性和不可更改性也變得愈來愈重要。因此，要安心、放心及有信心地享用資訊科技帶來的方便與貢獻的同時，更需要「網上監察員」採用有效的身份核證工具 - 「數碼證書」來保障使用者個人的資料及通訊的安全。

希望藉此手冊能為讀者提供網絡安全的檢測基礎資訊，以提高大家在應用互聯網作業時的警覺性，並且能善用互聯網為我們帶來的快捷與方便。



I'M CERTIZEN

NETIZEN

CITIZEN

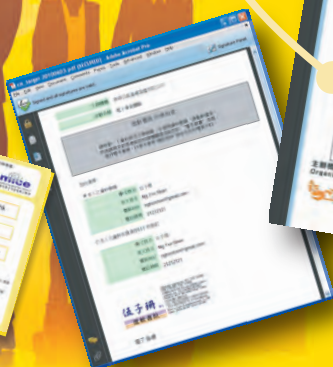
做個精明的 CERTiZEN

互聯網的開創，為使用者於虛擬世界裡建立了一個跨越地域界限，打破時空限制，包羅萬有的寶庫也改變了以郵遞傳送資訊的模式。可是，一些居心不良的不正當使用者，破壞了原本井井有條的網絡秩序。了解當前不正當的手法，可以喚起了用家的危機警覺性，作出預防措施，辨別網站的真偽，保障用戶的身份，成為網絡上真正的 **CERTiZEN**。

保障私隱
由**電子證書**開始
Protect Your Privacy
By e-Cert



機構認可人士在文件上以**電子證書簽署**，令文件更為真實可靠並得以永久保存，亦符合環保少用紙的原則。



為安全網絡通訊而設的「數碼證書」

利用互聯網溝通與服務 - 發放電子郵件、互換資料以及訂購貨品，已成為一般人日常生活的一部分。

為解決網上交易的保安，香港郵政成立香港第一家在《電子交易條例》（香港法例第553章）下的認可公共核證機關，以推動香港電子商務的發展。現時，香港郵政核證機關發出符合電子交易條例要求的「認可數碼證書」。根據《電子交易條例》，使用該條例下認可的數碼證書作出的數碼簽署與書面的簽署具同等法律效力。

採用核證機關認可的數碼證書有效認證網上身分，確保電子交易在安全及可信任的環境下完成，而其設立證書儲存庫及公開目錄，更方便市民進行網上交易前，查核對方的證書是否有效，令網上交易更為安全。

認證

► 核證進行電子交易雙方的身份；

完整

► 確保信息內容在傳送過程中未有被他人蓄意或無意更改；

不可推翻

► 確認雙方同意交易條件，防止任何一方否認曾作出承諾；和

機密

► 確保只有交易雙方才可得悉交易內容和資料，而不會被第三者竊取。



電子簽名時間章
法律保護最放心



電子簽名確真實
網絡交易有保障



防止對方不認責
交易受保防損失



電子交易條例下
網絡交易受保障



文檔資料都加密
私人重物免外洩



已簽資料不可改
資料真確防偽冒



網絡通訊實名制
有名有姓防冒認

「數碼證書」

實踐電子交易的

保安問題



甚麼是「公開密碼匙基礎建設」？

公開密碼匙基礎建設（公匙基建）是包括：

- 利用公開密碼匙加密技術（公匙加密技術）及
- 利用數碼證書，在公開的網絡（例如互聯網）上用作認證身份和接達控制的方法。

公匙基建是軟件、硬件、人員、策略和操作規程的總和，它們要完成創建、管理、保存、發放和廢止證書的功能。

公匙基建系統的建構

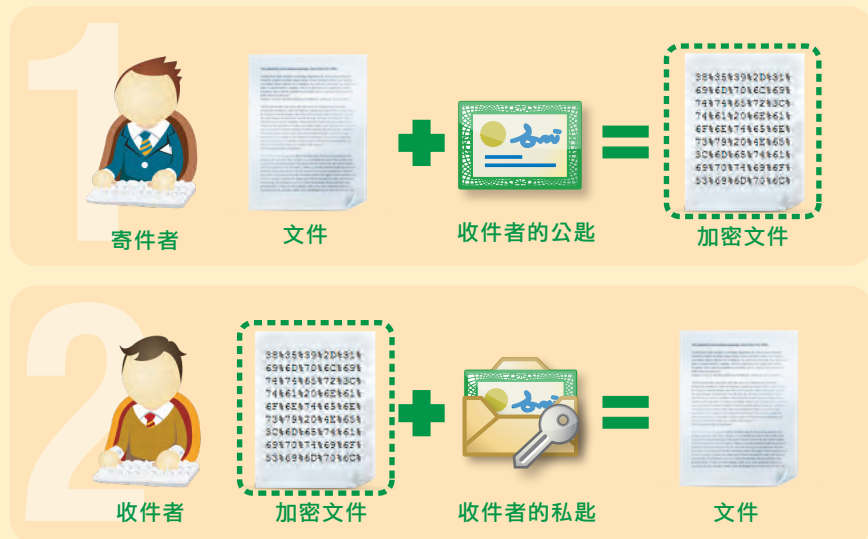


公匙密碼學

數碼簽署



電子證書加密

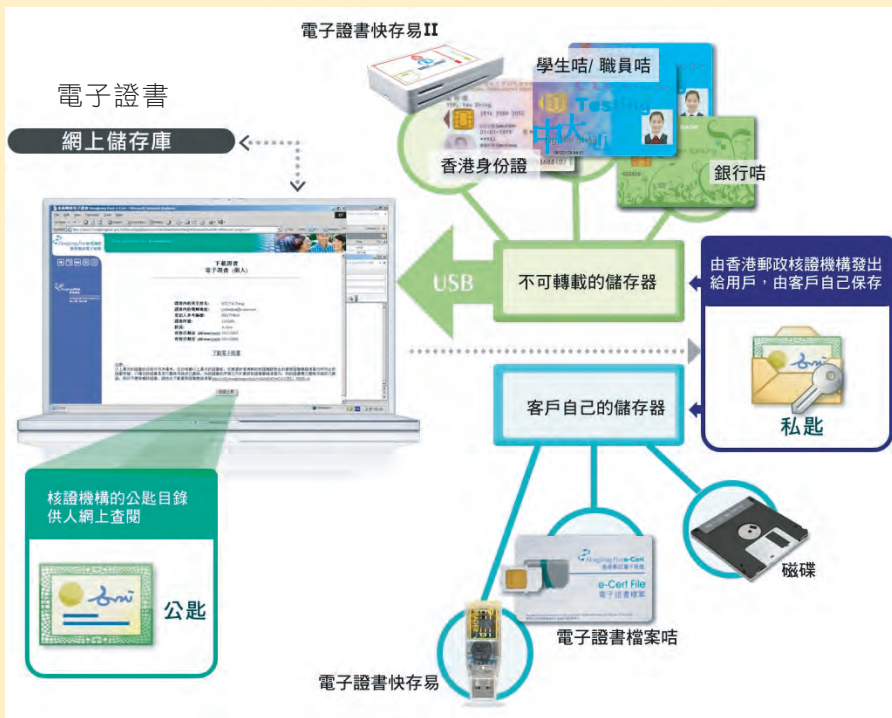


私人密碼匙(私匙) 和 公開密碼匙(公匙)

數碼證書是一份數碼文件，包含私人密碼匙(私匙)和公開密碼匙(公匙)來核證個別持有人的真正身份。

「私匙」屬用戶私有，由用戶自行保存，只有用戶自己才能使用。

「公匙」存放在認可核證機關的公開目錄內，所有人都可以查閱、索取及使用。透過網上查看可核證個別人士是否該公開密碼匙的真正持有人。



<http://www.hongkongpost.gov.hk>

網上身份的查證

認可核證機關網上儲存庫公佈
所有已被接納的證書。

例：在香港郵政電子核證的儲
存庫內可搜尋香港郵政電子核
證發出的電子證書。證書包含
一條公開密碼匙、用戶名稱、
有限期、證書編號及登記人參
考號碼。

在網上他是誰？
他的身份可以跟查
他的公司已備有商業登記
他的伺服器可查證

So easy!
就找到對方的身份與「公匙」



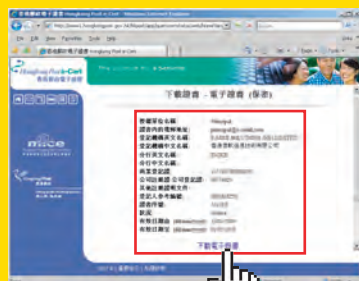
登入香港郵政核證機關網站，按
[搜尋及下載]



選擇搜尋及下載證書類別



輸入其中一項檢索要求，
如證書內的電郵地址



下載證書公匙

電子證書的種類



一個普通市民，可將電子證書儲存在身份證內

應用：日常文件保密，電子簽署，收發數碼簽署電子郵件，報稅，銀行交易，登記成為選民

申請種類：電子證書(個人)



一位公司主管、職員

應用：與其他公司進行交易，包括電子簽署，將合同保密，收發數碼簽署電子郵件

申請種類：電子證書(機構)



公司內部傳訊

應用：與公司內部同事進行電子傳訊而又需要簽章確認或將文件保密以防外洩

申請種類：電子證書(保密)



公司網站\網絡伺服器

頒發給香港特別行政區政府各局及部門、獲政府簽發有效商業登記證之機構以及獲香港法例認可之本港法定團體（"登記人機構"）。。

應用：減少受網路釣魚釣(盜)取網絡使用者的帳戶密碼及個人資料

申請種類：電子證書(伺服器)



電子證書的應用範例



香港公共圖書館

便捷的圖書館服務



運輸署

續領正式駕駛執照



樂滿郵網上購物

安全網上購物平台

電子證書

稅務局



輕鬆處理稅務問題

選舉事務處



選民登記



數碼簽署及有效驗證

辨別網站的真偽

數碼證書可應用在公共或商業服務，例如**安全電子郵件**、**網上政府公共服務**、**網上娛樂**、**網上買賣股票**或**網上銀行服務**，除此之外，亦適用於**電訊**、**娛樂**、**教育**及**醫療**等服務。只要你擁有數碼證書，便可安坐家中，使用安全、快捷的網上服務。

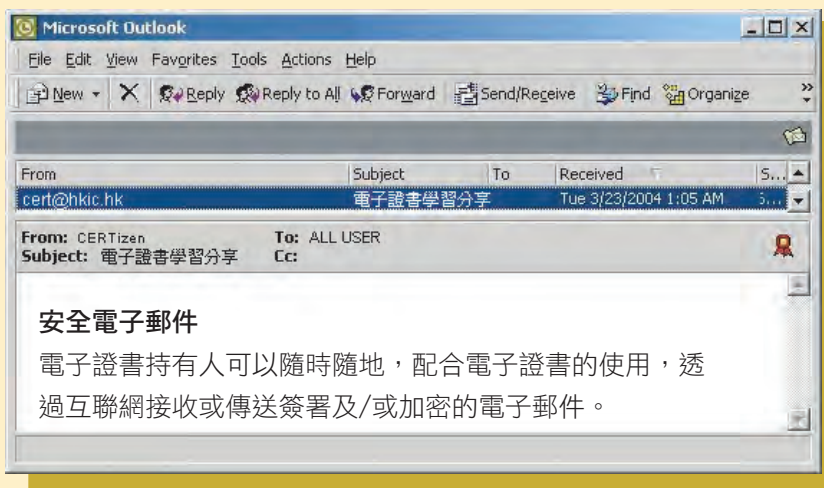


登入網站，見標誌，
按下查證真偽



標示為一安全網站

傳送安全電子郵件

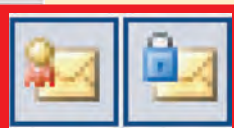
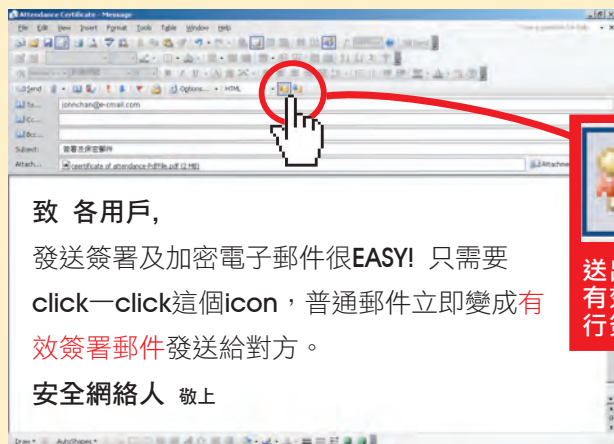


安全電子郵件

電子證書持有人可以隨時隨地，配合電子證書的使用，透過互聯網接收或傳送簽署及/或加密的電子郵件。

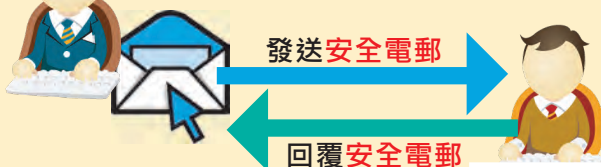
數碼簽署提供認證完整性及不得毀約的承諾。

有效驗證安全電郵



送出郵件前以真實有效的數碼證書進行簽署及加密

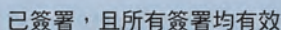
採用有效的「數碼證書」發送簽名及或加密郵件



收件人利用自己的「私匙」打開一封已簽名及加密的郵件



標示指郵件是經真實及有效的數碼證書進行簽署及加密



數碼簽署是利用非對稱密碼技術及雜湊函數，將該電子記錄作數據變換而產生。程式計算出信息的數值，把數值用私匙加密，當指定人收到訊息後，用簽署人的公匙把數值解密，然後檢查信息與數值是否相對應，如是相對應，便證明簽署人的身份，及證明信息內容是沒有被篡改。數碼簽署和手寫簽署具有相同樣的法律效力。

總監

香港新一代文化協會科學創意中心

Digitally signed by WONG Kam Yiu Jimmy
DN: c=HK, o=Hongkong Post e-Cert(Organisational),
ou=0001876679,
ou=000000000000000000000000HKGNCALCHAPTER-112,
ou=HONG KONG NEW GENERATION CULTURAL
ASSOCIATIONLIMITED,
ou=SCIENCE INNOVATION CENTRE,
email=djwong@newgen.org.hk, cn=WONG Kam Yiu Jimmy
Date: 2010.04.30 11:10:35 +0800"

電子簽署的作用是供收件人確認您的身分，並確定訊息於發送過程未經更改，簽署後即表示同意該內容，效能如同手寫簽署不可抵賴或推翻。



數碼證書簽署及有效驗證

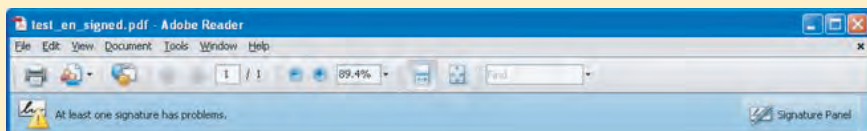
經數碼簽署的文件，具備一定的特徵。當使用**Adobe Reader 9.0**版或**Adobe Acrobat 9.0**版開啟文檔，電腦將顯示該檔案包含一個數碼簽署，通過檔案頂部的藍色色帶顯示檔案的真確性和有效性。讀者更可進一步檢查數碼簽署，以便追溯檔案的來源。



有效簽署



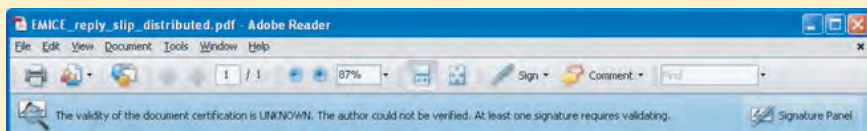
表示檔案內容未經任何篡改。同時，若彈出視窗或藍色色帶顯示數碼簽署有效的消息，表明核證機關知道檔案作者的身份，且其數碼簽署是真實有效的。



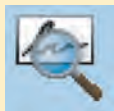
無效簽署



表示檔案的數碼簽署不可靠，或檔案已被篡改。作者的數碼證書可能因為某種原因被撤銷，或已過期。無論如何，收件人應拒絕任何包含無效數碼簽署的檔案。



未知作者



有兩個含義：數碼簽署因為網絡連接問題無法驗證，或數碼簽署無法通過互聯網立即得到認證。如果看到此消息，請確認您的電腦已正確連接至互聯網。如果數碼簽署仍然無法驗證，應拒絕此檔案。

給用戶的小測試

1. 在香港認可核證機關是否受香港政府資訊科技總監辦公室監管？

- a. 是
- b. 不是

2. 在香港，認可核證機關發出的認可「數碼證書」是受甚麼條例約束？

- a. 電子交易條例
- b. 交易條例

3. 甚麼是「數碼證書」？

- a. 由核證機關發出及數碼簽署的電子文檔，以核實證書持有人之身分
- b. 是一般的電子文檔

4. 從那裡可核證認可「數碼證書」持證人的身份？

- a. 可從認可核證機關的儲存庫中查詢
- b. 無法查核

5. 「數碼證書」的私匙是由誰人保管？

- a. 由證書持有人保管
- b. 從認可核證機關的儲存庫中下載

6. 如何獲得他人數碼證書的公匙？

- a. 由證書持有人保管
- b. 從有關認可核證機關的儲存庫中下載

7. 要採用「數碼證書」進行簽署，簽署人是否必須備有「私匙」？

- a. 是
- b. 不是

8. 收件人能用自己的私匙打開發件人以「數碼證書」加密的郵件嗎？

- a. 可以
- b. 不可以



監管條例及守則

電子交易條例

<http://www.ogcio.gov.hk/chi/eto/ccap553.htm>

認可核證機關業務守則

<http://www.ogcio.gov.hk/chi/caro/csub3.htm>

香港郵政電子證書核證作業準則

http://www.hongkongpost.gov.hk/product/cps/ecert/img/cps_cn27.pdf

個人資料（私隱）條例

<http://www.pcpd.org.hk/chinese/ordinance/ordglance.html>

人事登記條例

<http://www.legislation.gov.hk/chi/index.htm>

官方機密條例

<http://www.legislation.gov.hk/chi/home.htm?SearchTerm=%u5B98%u65B9%u6A5F%u5BC6%u689D%u4F8B>

主辦機構

香港公匙基建論壇

Hong Kong Public Key Infrastructure Forum Ltd

支持機構

政府資訊科技總監辦公室

Office of the Government Chief Information Officer

香港郵政電子核證

Hongkong Post e-Cert

恒生銀行

Hang Seng Bank

香港億軟信息技術有限公司

E-Mice Solutions (H.K.) Limited

互聯網專業協會

iProA

香港電腦學會

Hong Kong Computer Society

香港新一代文化協會科學創意中心

Hong Kong New Generation Cultural Association
Science Innovation Centre

協通科技有限公司

LetLink Technology Limited

如欲提供意見，歡迎登入 <http://www.hkic.hk>

筆記

筆記

筆記

筆記

www.hkic.hk



{新世代} 安全網絡人

CERTIZEN www.hkic.hk

在社區更廣泛應用數碼證書及採用公匙基建科技
Wider Usage of Digital Certificate and Adoption of PKI Technology in the Community

The information contained here is for reference only. The owner, "Hong Kong Public Key Infrastructure Forum Ltd", is not liable for errors, omissions or inadequacies in the information provided. The readers assume sole responsibility for using the information to achieve their own purposes.

於本手冊載述的資料僅作參考用途。本刊物的版權人「香港公匙基建論壇有限公司」對所提供資料的錯漏或不足一概不負上任何責任。讀者若運用本手冊資料在履行其個人目的時，應當為自己的行為負上全責。