端對端加密之金鑰安全儲存方式

作者/張鴻仁

提要

一、網路的普及讓駭客產業有了舞台，於是資料安全(訊息、語音、檔案等的加密以及來源性驗證)成為了基本需求。

二、資料安全從早期的用戶端到伺服器端加密轉而追求只有通訊雙方能解讀的端對端加密，在端對端加密的機制下，任何一方(包含通訊軟體伺服器)也都無法從中竊取通訊雙方的傳訊資訊。

三、本文提供了一種貼膜的方式讓行動裝置能透過實體載具提供的公開金鑰基礎架構功能，能避免通訊伺服器的偽冒；也提供了以憑證換憑證的方式，能將資料安全延伸到其它平台，並且仍維持著不被偽冒的特性。

關鍵詞：資料安全、端對端加密、金鑰、公開金鑰基礎架構

前言

網路普及以來，即時通訊軟體從桌上型電腦的ICQ、MSN發展到現在智慧型手機上的LINE、Skype、微信等，將人們利用傳統電信服務來撥打電話、傳送簡訊的習慣，迅速轉為使用通訊軟體的服務來進行更豐富的社交行為如傳送多媒體檔案、視訊等。現在熟悉的即時通訊軟體，都是從西元2010年(民國99年)前後發展起來的[1]，從國家通訊傳播委員會(National Communications Commission，NCC)所公開的資料[2]也可看到，簡訊的發送量從2012年的最高峰85億則一路下降到2017年的39億則，隨後才又因為一次性動態密碼((One Time Password，OTP)認證需求以及這二年來簡訊實名制再度達到高峰；傳統的電信通話時間也是從2012年的最高峰432億分鐘逐年降到2021年的102.9億分鐘。二份參考資訊彼此呼應了現代在簡訊上的應用在廣告、認證以及實名制的應用佔大宗，個人社交的平台已大量轉移到行動裝置上的即時通訊軟體。

早期的即時通訊軟體採用的是用戶端到伺服器端(Client to Server，C2S)加密傳輸，所有網路上傳送的訊息雖然安全，但是對於伺服器端而言卻是赤裸裸的明文。在大眾對於安全及隱私的意識上漲，端對端加密更加受到青睞，它能提供只有雙方才能加密、解密的通訊方式，即使訊息備份在伺服器端，也無法被伺服器取得明碼內容。現行著名的即時通訊軟體如Line (LINE Letter Sealing)以及WhatApp (Signal Protocol)於2016年、Skype (Signal Protocol)於2018年相繼推出支援端

[1] “時代的眼淚！曾經的霸主MSN跟即時通，為何被LINE及Messenger超車？”https://blog.simpleinfo.cc/shasha77/history-of-instant-communications-software-yahoomessenger-msn-line-facebookmessenger （ 檢索日期：2022年7月12日）

[2] “國家通訊傳播委員會 - 開放資料集列表 – 行動通訊業務平均每月簡訊量 /行動通訊業務平均每月通話時間”https://www.ncc.gov.tw/chinese/opendata.aspx?site_content_sn=3507 （ 檢索日期：2022年7月14日）

對端加密功能[3]。

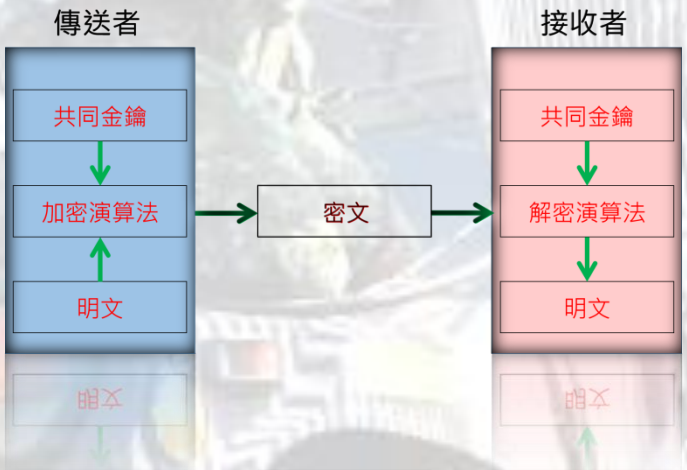
資料安全概述

資料安全指的是資料的隱密性以及不可否認性。隱密性要求資料的傳送需要被加密，沒有金鑰的其它人無法解密還原資料內容；不可否認性則訴求資料來源的無法被偽冒。基於資料加解密的效率考量，加解密多是採取「對稱式金鑰」演算法如三重數據加密演算法(Triple Data Encryption Algorithm，Triple-DES)、進階加密標準（Advanced Encryption Standard，AES）；不可否認性則是靠「非對稱式金鑰」演算法來完成。在端對端加密機制下，「對稱式金鑰」是透過「金鑰協商」機制來取得，目前多是使用橢圓曲線迪菲-赫爾曼密鑰交換演算法（Elliptic Curve Diffie–Hellman key exchange，ECDH）。

一、對稱式/非對稱式(金鑰)演算法

對稱式金鑰意指通訊雙方，彼此掌握相同的金鑰資訊，雙方皆是使用同一個金鑰資訊進行加解密，其架構如圖1。因為對稱式加解密演算法的速度上，比非對稱式演算法快上許多，因此若要進行大量資料的加解密，通常被列為不二選擇。在速度與安全性上的考量，目前多使用AES[4] 。

圖1 對稱式加解密



資料來源:作者自繪

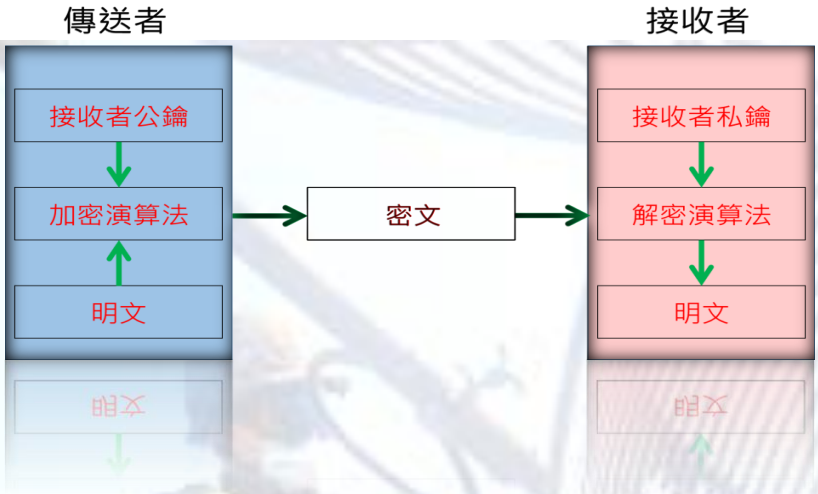
非對稱式金鑰則是每位使用者持有一對公私鑰，私鑰由使用者自己安全持有；公鑰則公開讓其它使用者取得。加密後的密文是使用接受者公開的公鑰搭配非對稱式演算法(加密)進行運算後取得，解密後的明文則只能由接收者使用自己的私鑰搭配非對稱式演算法(解密)運算後取得，其架構

[3] "點對點加密通訊協定之前瞻技術與探討.pdf"http://www.twisc.org/tw/wp-content/uploads/2020/09/%E9%BB%9E%E5%B0%8D%E9%BB%9E%E5%8A%A0%E5%AF%86%E9%80%9A%E8%A8%8A%E5%8D%94%E5%AE%9A%E4%B9%8B%E5%89%8D%E7%9E%BB%E6%8A%80%E8%A1%93%E8%88%87%E6%8E%A2%E8%A8%8E.pdf （ 檢索日期：2022年7月26日）

[4] 蔡定國, AES密碼演算法在多核心處理器環境之設計和實作,中華大學資訊工程學系碩士班論文,中華民國100年8月, 頁1

如圖2。

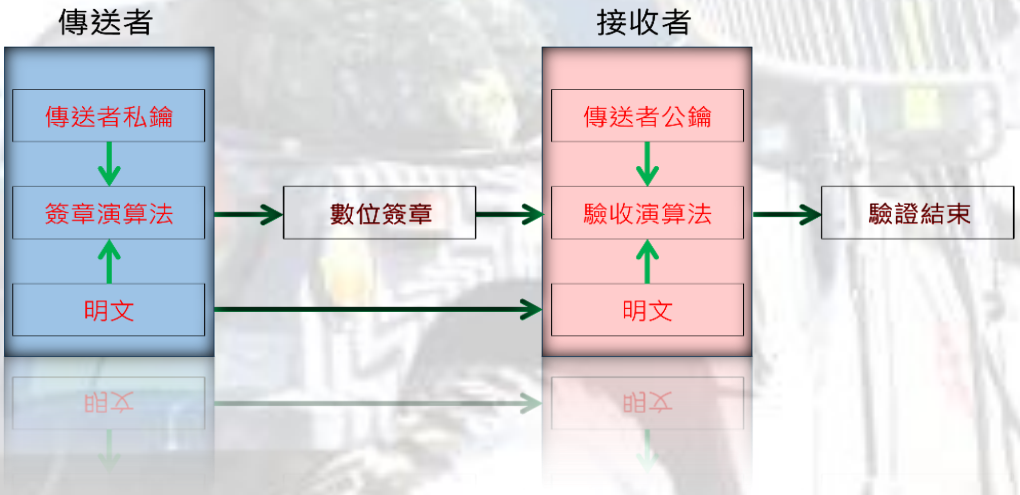
圖2 非對稱式加解密



資料來源:作者自繪

非對稱式金鑰的特性，又能延伸出數位簽章以及金鑰協商的應用。數位簽章的產生，是由傳送者使用自己的私鑰搭配非對稱式演算法(簽章)針對要傳送的明文製作出一個無法被偽冒的產出物。其它使用者都能夠使用傳送者公開的公鑰搭配非對稱式演算法(驗章)來針對收到的明文進行來源性驗證，其流程如圖3。

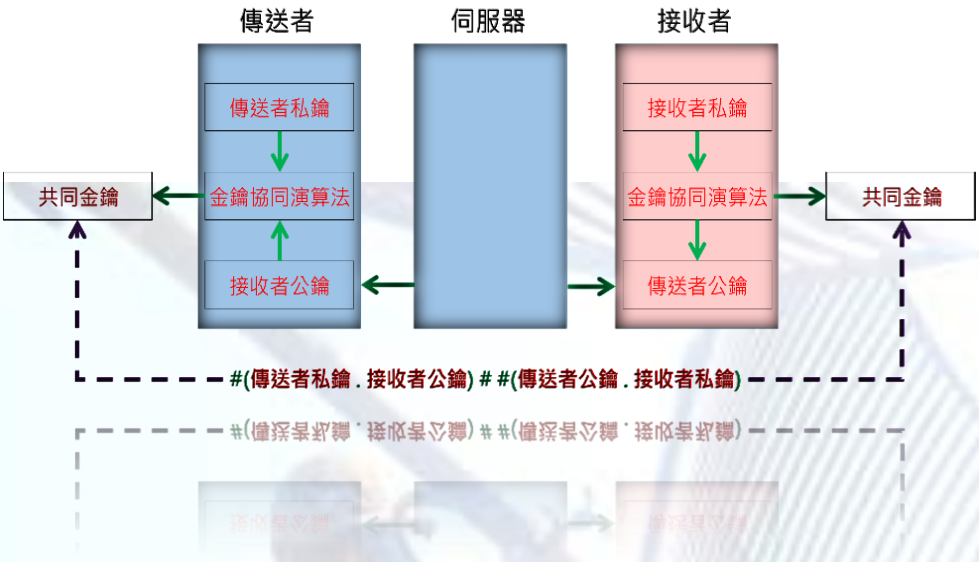
圖3 簽驗數位簽章



資料來源:作者自繪

金鑰協商則是由傳送者與接收者要進行大量資料加解密前，分別使用自己的私鑰與對方公開的公鑰搭配非對稱式演算法(金鑰協商)及其它資訊計算出相同的共同金鑰，其流程如圖4。

圖4 金鑰協商

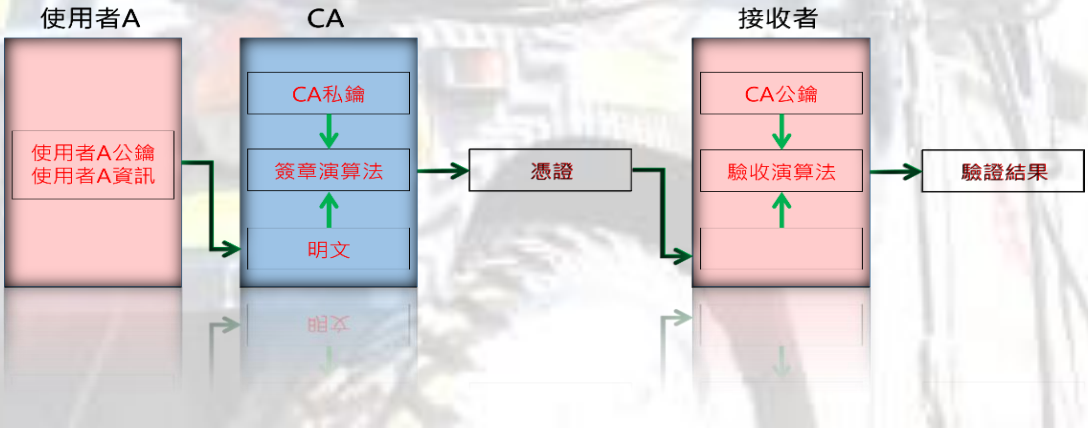


資料來源:作者自繪

二、公開金鑰基礎架構 (Public Key Infrastructure，PKI)

在網路的世界，多數時候人與人並無法直接面對面，如何確定與你交換訊息的另一方的身分是一個困難的課題，而這個課題可藉由公開金鑰期礎建設來解決。公開金鑰期礎建設利用了非對稱式金鑰的特性，首先建立一個眾人信任的角色名為憑證管理中心 (Certificate Authority，CA)，它自行產製一對公私鑰，並公開它的公鑰作為所有人的信任基礎。日後，每個使用者自行產製各自的公私鑰，並將使用者資訊以及公鑰交付憑證管理中心，憑證管理中心則將針對各個使用者的資訊及公鑰製作出屬於該使用者的數位簽章 (後續稱之為憑證)並供各個使用者可取得進而驗證其它使用者之身分以及該使用者產製之數位簽章，其架構如圖5。

圖5 公開金鑰基礎架構之使用



資料來源:作者自繪

三、端對端加密

透過公開金鑰礎建以及非對稱式演算法的特性，通訊的雙方或者多方可以建立起只有彼此間能加解密的通訊安全，也能夠提供通訊來源的保障。以通訊雙方為例，彼此首先透過憑證確

認彼此身分，接著利用金鑰協商方式計算出對稱式金鑰供資料傳遞時的加解密使用，且可額外透過自身的私鑰針對資料產出相對應的數位簽章供另一方驗證。

現行即時通訊軟體在資料安全上的介紹

現行知名的即時通訊軟體如Skype、Telegram、Line等等雖然在功能上都有不同的差異點(如Telegram的閱後即焚、Line的簡訊收回、群組通話等)，但在資料安全上都已支援端對端加密。下面將介紹幾個即時通訊軟體在金鑰對的註冊方法，並不細談如何實際進行端對端加密。

一、LINE

是韓國的Naver集團旗下的LINE 株式會社的即時通訊軟體。Line於2016年宣佈支援端對端加密技術LINE Letter Sealing。當Line應用程式第一次啟動或者Letter Sealing功能每一次被啟動(前一次功能關閉後)時會產生出金鑰對，它使用橢圓曲線迪菲-赫爾曼金鑰交換演算法，並將該公鑰傳送至伺服器端作註冊[5]。即使對話資料是以加密（連LINE也不能解密）方式存放在LINE的伺服器，金鑰是只有收發兩端才有，且不會轉送出這兩端以外。前提是我們必須「信任」LINE在任何時候都會遵守，而且，由於是國外公司，須時時留意是否因股權所有權轉移，而改變其公司主要資安的政策或執行。

二、Skype、WhatsApp

Skype與WhatsApp在端對端加密技術都採用Signal Protocol[6]，但在部份商用邏輯上具有些微差異，例如WhatsApp提出主要裝置(Primary device)以及配套裝置(Companion device)概念；Skype則每個裝置彼此間都是獨立的。

WhatsApp在2014年二月被臉書以美金119億收購。2016年宣布WhatsApp使用端對端加密在任何一種通訊形式(文字/語音/影片等)，WhatsApp在主要裝置(Primary device,可以是Android/iPhone)第一次安裝註冊時會產出ECDH金鑰對，並將該公鑰傳送至伺服器端作註冊。配套裝置(Companion device， 不可為Android / iPhone)所產生之ECDH金鑰對則是透過主要裝置上之私鑰作保證(對配套裝置所產製的公鑰作數位簽章)，並把該公鑰傳送至伺服器[7] 。

Skype 在2011年被微軟公司以美金85億收購。Skype 使用的「基於 IP 的語音傳輸（VoIP)」 專有軟體為 Skype protocol。微軟收購後，新的專有軟體稱為 Microsoft Notification Protocol 24。. 從2018年8月開始，Skype在所有平台都有提供端對端加密，Skype則是在每一個裝置的登入時，會產製ECDH金鑰對[8] ，並將該公鑰傳送至伺服器端作註冊以利後續端對端加密使

[5] “LINE Encryption Overview Technical Whitepaper”https://scdn.line-apps.com/stf/linecorp/en/csr/line-encryption-whitepaper-ver2.0.pdf（檢索日期：2022年7月30日）
[6] “VoIP and Skype Security” https://www.researchgate.net/publication/337590520_VoIP_and_Skype_Security （檢索日期：2022年8月1日）
[7] “WhatsApp Encryption Overview” https://vdocs.ro/doc/whatsapp-security-whitepaper-v4-preview-3md8dk2dq3 （檢索日期：2022年8月1日）
[8] “What are Skype Private Conversations” https://support.skype.com/en/faq/FA34824/what-are-skype-private-conversations?q=signal （檢索日期：2022年8月4日）

用[9]。

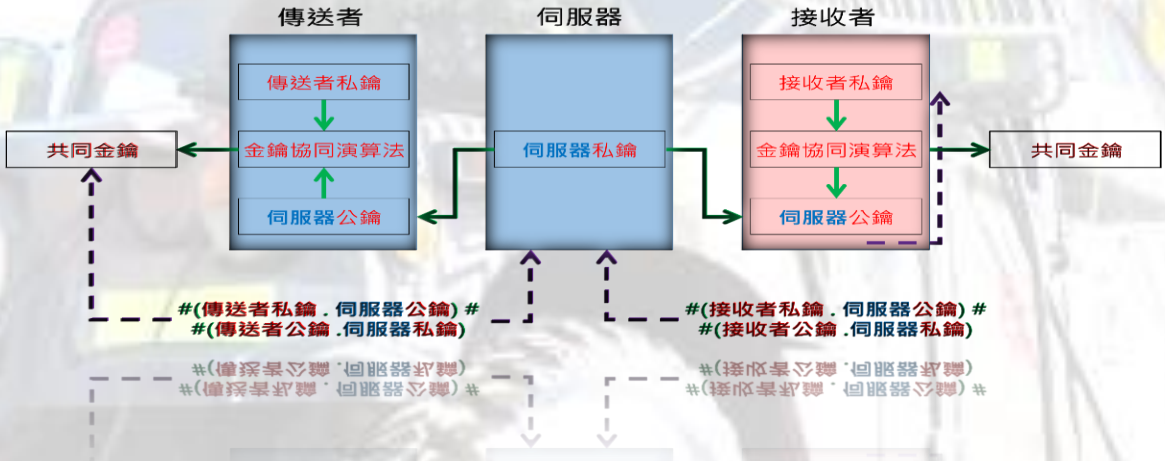
三、Telegram

由俄羅斯人Pavel Durov和Nikolai Durov創立，公司位於倫敦。Telegram的用戶端的程式是開放源碼。Telegram在每一個裝置的安裝註冊時，會產製金鑰對，並將該公鑰傳送至伺服器端作後續與伺服器的安全通道建立。與其它即時通訊軟體的不同在於，它金鑰協商的部份是使用RSA 2048[10]，並且在與其它使用者進行端對端加密時，並不是使用註冊在伺服器端的公鑰來產生端對端加密的輸入值，而是使用臨時產生的金鑰對(因此它提供了Perfect Forward Secrecy特性)[11]。

運用薄膜貼片卡在資料安全上的介紹

現行的即時通訊軟體雖具有端對端加密功能，即使都是端對端加密，使用哪一種端對端加密機制也會影響安全性，並不是每一種端對端加密機制都一樣安全。而且，端對端加密還是有遭受中間人攻擊的危險，這也是為什麼端對端加密應該要搭配身份認證機制才更加安全。但因為同一帳號所持有通訊裝置所產生出金鑰對的公鑰各有不同，故通訊的雙方只能透過對伺服器的信任進而相信通訊的另一方身分。在這種情況下，一個受入侵的伺服器是可以自行產製金鑰對，並且冒充一位合法的使用者與其它使用者進行通訊(偽冒身分)；或者在要進行通訊的雙方建立安全通道時，自行產製金鑰對並丟向雙方，充當雙方在金鑰協商過程中的公鑰，進行中間人(Man in the Middle)攻擊以取得雙方的通訊內容，其架構如圖6。

圖6 伺服器進行中間人攻擊監聽通訊



資料來源:作者自繪

[9] "Skype Private Conversation Technical white paper" https://az705183.vo.msecnd.net/onlinesupportmedia/onlinesupport/media/skype/documents/skype-private-conversation-white-paper.pdf （檢索日期：2022年8月4日）
[10] 維基百科 https://zh.wikipedia.org/wiki/Telegram （檢索日期：2022年9月1日）
[11] "MTProto Mobile Protocol" https://core.telegram.org/mtproto （檢索日期：2022年8月5日）

一、使用薄膜貼片卡

端到端加密並不能避免終端本身的安全風險。每個使用者的電腦等裝置上仍然存在金鑰被盜（以進行中間人攻擊），或是被解密的資訊被讀取的可能性，要避免伺服器進行中間人攻擊或者偽冒身分，架構上需要避免「無條件信任」使用者所屬的公鑰。提升端點安全性最簡易的方式是使用者持有一張晶片卡 (支援PKI功能，能產製金鑰對並且擁有私鑰不被輸出的特性)，屬於使用者的公鑰在公開金鑰基礎建設中被憑證管理中心所認證供所有其它使用者得以信任，如此一來使用者能確信通訊的對象的身分，並且不會有伺服器偽冒身分或進行中間人攻擊的機會。實現在手機即時通訊軟體的作法，可以是一張支援PKI功能的薄膜貼片卡，將之貼在一般使用者身分模組（Subscriber Identity Module，SIM）上讓即時通訊軟體可藉由該薄膜貼片卡進行安全通訊。

薄膜貼片卡是晶片卡的一種封裝方式，其架構如圖7，內含一個支援PKI功能的程式(Applet)，該Applet除了有自行定義的智慧卡傳送命令(Application Protocol Data Unit，APDU)外，也支援對於一般SIM卡APDU的通透能力以維持一般SIM卡在手持裝置上的功能。在安全性上，薄膜貼片卡內之晶片應符合全球平台組織（Global Platform，GP)規範實作，並且經過安全評估共通準則(Common Criteria，CC)及聯邦資訊處理標準(Federal Information Processing Standards，FIPS)等之國際認證以避免在安全性上的疏露。Applet之設計也都是功能導向的設計，只有提供功能需求的APDU，故駭客也無法針對卡片內作業系統進行攻擊。在CC及FIPS認證的基礎上，卡片內金鑰及憑證的存取、金鑰分析功擊等獲得了高度的檢驗，故金鑰的儲存較手持置有著更高的安全性。

圖7 晶片結合薄膜貼片卡

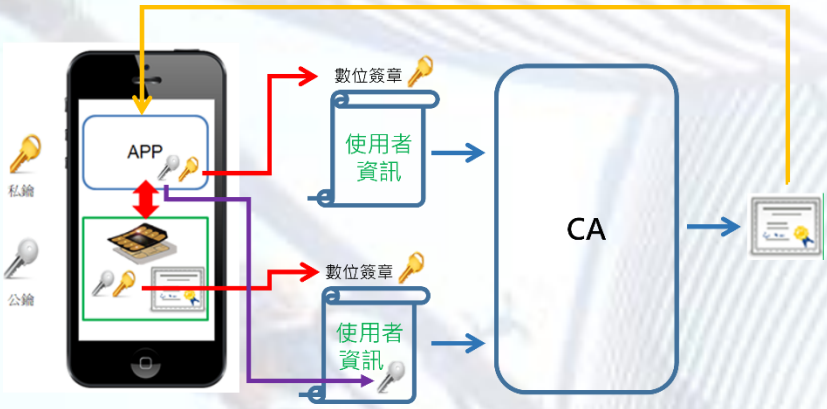
資料來源:作者自繪

二、以(憑)證換(憑)證

使用薄膜貼片卡的優點在於更換手機後即時通訊軟體不需要再進行金鑰對的產生，可以直接延用薄膜貼片卡內的金鑰對。若要提供現行即時通訊軟體的多裝置使用，則可以進行以證換證的動作， 做為在其它裝置上金鑰對的串鏈信任。首先，其它裝置上的即時通訊軟體產製金鑰對後使用私鑰簽出憑證請求檔(Certificate Signing Request，CSR)，再透過薄膜貼片卡內的私鑰對即時通訊軟體產製的公鑰資訊產出數位簽章，再將憑證請求檔以及數位簽章交付憑證管理中心作認證，

最後從憑證管理中心取得針對即時通訊軟體產製的公鑰的憑證，其流程如圖8。在通訊的建立時，其它使用者可透過該憑證確信該公鑰屬於該使用者。

圖8 以(憑)證換(憑)證



資料來源:作者自繪

三、與現行即時通訊軟體比較與分析

本文所提供之方法，能在端對端加的基礎上提供更高的信任安全，杜絕惡意或遭入侵的伺服器進行攻擊，詳細比較請參考表1。

表1 現行即時通訊軟體與本方案之比較表

現行即時通訊軟體與本方案之比較表		
	金鑰由即時通訊軟體產生	金鑰由薄膜貼片產生
成本	✓ 低。可使用智慧型裝置提供之金鑰產製及儲存功能，不需要額外購買硬體設備。	✓ 稍高 。需購買薄膜貼片卡或者使用近距離無線通訊(Near-Field Communication，NFC)卡片搭配手機 NFC，亦可使用一般晶片卡搭配讀卡機。
可攜性	✓ 高。全部使用手機提供之功能及空間	✓ 略低。若是使用薄膜貼片則可攜性高，若是使用其它實體卡片，可攜性略低。但若搭配以(憑)證換(憑)證的一次性動作，可攜性與目前即時通訊軟體一樣高。
信任安全性	✓ 略低。因為使用者無條件信任伺服器所提供的使用者資訊與金鑰對照關係，使用者無法避免受到惡意或受入侵的伺服器欺騙	✓ 高。使用者所信任的來源是憑證管理中心所發出之該使用者的憑證，在切換裝置時採用的仍是同一張憑證。若是在多裝置的情況下，搭配以(憑)證換(憑)證的方法，每一個其它裝置的金鑰仍然受到憑證管理中心認證，確保是該使用者之金鑰。
金鑰安全性	✓ 金鑰儲存的安全性取決於手機作業系統的安全性，以及駭客技術的進步。	✓ 薄膜貼片卡或晶片卡內之 Applet 所提供與外界動作的 APDU 為功能導向，並無法進行任意的嚐試存取。

資料來源:作者自繪

結論與建議

隨著大眾的安全與隱私意識上漲，端對端加密就成為了一種更受歡迎的加密方式。這是一種只有收發訊息兩端可以加密與解密訊息的溝通方式，優點是解密後的訊息只會保存在用戶端，安全性跟隱私性較高，所以目前很多通訊軟體都主打端對端加密通訊。端對端加密旨在讓通訊內容不被其它人所知悉，用戶間傳送的訊息只有真正的訊息發送方和收信方能讀取。不管是第三者想從中竊聽或是平台經營者都無法讀取。而且，保護的訊息包括文字訊息、群組、圖、影音和附加檔。本文分析現行即時通訊軟體白皮書後提出安全疑慮及建議作法以提昇安全性。尤其是近年來，各國對於來自中國大陸的駭客或網軍攻擊事件一直未曾中斷過。而同樣面臨中共高度威脅的臺灣，遭受中共網軍攻擊的情況非常嚴重，對象當然是以政府機關及軍事單位為首要目標，因應中共駭客入侵風險升高目前國軍對於各級部隊奉准辦理智慧型手機試行作業，應避免透過社群媒體、通訊軟體談論敏感公務或傳輸公文資料，以建立各級部隊強化官兵資安觀念及安全警覺，這是一個良好的開始，但是為因應高科技帶來的智慧型手機通訊便利性與即時性，國軍需要積極對安全通訊擬定出一套整體規畫與辦法，以建立一個可靠，可稽核的機制來保護我軍的通訊和重要機密。因為目前常用的網路平台，如 Facebook, Google, LINE, Apple, 其雲端伺服器都在國外，通訊軟體服務商會不會配合政府要求交出使用者資料就是一個重要的考量點，為了不要將國軍之通訊機密受制於外國機構，我們建議解決對策是國人自主發展一套秘密通訊平台，在零信任的既有行動通訊網路上，搭配一張支援PKI功能的薄膜貼片卡，將之貼在一般SIM卡上，讓即時通訊軟體可藉由該薄膜貼片卡進行安全通訊。建構一套安全的、不被竊聽的通訊系統，完成「端點端」的加密通訊，方能確保機密不外洩，維持國家安全與國防戰力。

參考文獻

一、“時代的眼淚！曾經的霸主MSN跟即時通，為何被LINE及Messenger超車？” https://blog.simplei nfo.cc/shasha77/history-of-instant-communications-software-yahoomessenger-msn-line-facebookmessenge r（檢索日期：2022年7月12日）

二、“國家通訊傳播委員會 - 開放資料集列表 – 行動通訊業務平均每月簡訊量 /行動通訊業務平均每月通話時間” （檢索日期：2022年7月14日）https://www.ncc.gov.tw/chinese/opendata.aspx ?site_content_sn=3507

三、“點對點加密通訊協定之前瞻技術與探討.pdf” http://www.twisc.org/tw/wp-content/uploads/2020/09 /%E9%BB%9E%E5%B0%8D%E9%BB%9E%E5%8A%A0%E5%AF%86%E9%80%9A%E8%A8%8A %E5%8D%94%E5%AE%9A%E4%B9%8B%E5%89%8D%E7%9E%BB%E6%8A%80%E8%A1%93% E8%88%87%E6%8E%A2%E8%A8%8E.pdf（檢索日期：2022年7月26日）

四、蔡定國, AES密碼演算法在多核心處理器環境之設計和實作,中華大學資訊工程學系碩士班論文 ,中華民國100年8月,頁1

五、LINE Encryption Overview Technical Whitepaper”https://scdn.line-apps.com/stf/linecorp/en/csr/line-encryption-whitepaper-ver2.0.pdf（檢索日期：2022年7月30日）

六、VoIP and Skype Security”https://www.researchgate.net/publication/337590520_VoIP_and_Skype_Security（檢索日期：2022年8月1日）

七、“WhatsApp Encryption Overview”https://vdocs.ro/doc/whatsapp-security-whitepaper-v4-preview-3md8dk2dq3（檢索日期：2022年8月1日）

八、What are Skype Private Conversations”https://support.skype.com/en/faq/FA34824/what-are-skype-private-conversations?q=signal（檢索日期：2022年8月4日）

九、“Skype Private Conversation Technical white paper”https://az705183.vo.msecnd.net/onlinesupportmedia/onlinesupport/media/skype/documents/skype-private-conversation-white-paper.pdf（檢索日期：2022年8月4日）

十、維基百科 https://zh.wikipedia.org/wiki/Telegram（檢索日期：2022年9月1日）

十一、“MTProto Mobile Protocol”https://core.telegram.org/mtproto（檢索日期：2022年8月5日）

作者簡介

張鴻仁，學歷：台灣大學電機工程碩士，任職中華電信研究院通資安全研究所高級研究員。