

出國報告（出國類別：開會）

2019 年國際安全印刷人會議

服務機關：中央印製廠

姓名職稱：廖郁琍 第二工廠副股長

劉文心 第一工廠工程師

派赴國家：丹麥

出國期間：108 年 10 月 20 日至 10 月 27 日

報告日期：109 年 1 月 21 日

摘 要

本屆 2019 年國際安全印刷人會議（SecurityPrinters）於 10 月 22 日至 25 日在丹麥哥本哈根之 Bella Center 舉行，共有來自世界各國 900 多位參與者與 70 多位演講者參加，以及 90 家世界知名供應商參展，藉由一系列有關安全印刷產業之議題研討、案例研究與技術展示，互相交流學習。

會議分為「鈔券（Banknote）」和「身分文件（Identity）」兩大主題，議程分為「鈔券及身分證明文件高階安全印刷人會議」、「鈔券及身分證明文件安全印刷人研討會」及「展覽」三大部分，主要針對防偽科技、防偽設計、防偽鑑識、偽造趨勢、廠房規劃及邊境管理等議題進行研討，本報告則根據議程中與本廠業務相關之議題，擷取匯整為下列八項主題：

- 一、身分和金錢的未來
- 二、鈔券改版跟設計
- 三、建置新廠房
- 四、科技應用－將手機運用於鈔券推廣
- 五、愛沙尼亞晶片身分證 ROCA 安全漏洞之經驗與教訓
- 六、區塊鏈對安全識別的潛在影響－於電子投票之應用
- 七、更加安全的馬爾他 eID 和 ePASSPORT
- 八、ISO 14298 安全印刷流程管理認證

此外，亦提出下列心得與建議，以期對本廠有所助益：

- 一、持續派員參加相關國際會議
- 二、進行各式軟硬體設備更新準備
- 三、加強員工資訊訓練
- 四、及早投入護照 PC 資料頁之研發與規劃

目 次

壹、前言	1
貳、目的	2
參、會議過程	
一、會議簡介	3
二、會議議程	5
肆、會議內容	
一、身分和金錢的未來	7
二、鈔券改版跟設計	9
三、建置新廠房	19
四、科技應用－將手機運用於鈔券推廣	26
五、愛沙尼亞晶片身分證 ROCA 安全漏洞之經驗與教訓	30
六、區塊鏈對安全識別的潛在影響－於電子投票之應用	45
七、更加安全的馬爾他 eID 和 ePASSPORT	53
八、ISO 14298 安全印刷流程管理認證	61
伍、心得與建議	
一、持續派員參加相關國際會議	74
二、進行各式軟硬體設備更新準備	74
三、加強員工資訊訓練	75
四、及早投入護照 PC 資料頁之研發及規劃	75

圖目次

圖 3-1	本次會議地點 Bella Center Copenhagen.....	4
圖 3-2	會場集錦.....	6
圖 4-2-1	2000~2018 年港幣各面額票面總額(左)及各面額流通張數(右)變化.....	9
圖 4-2-2	新版港幣正、背面之功能性規畫.....	10
圖 4-2-3	不同銀行所發行之新版一千元港幣.....	10
圖 4-2-4	協助視障人士辨識港幣面額之 App—讀鈔易使用畫面.....	11
圖 4-2-5	巴哈馬近十年鈔券被偽造率.....	14
圖 4-2-6	歐元發行數量及年增率.....	15
圖 4-2-7	歐元交易以筆數(左)及金額(右)顯示之支付方式比率.....	16
圖 4-2-8	歐洲各國銷售點交易的現金所占比率.....	16
圖 4-2-9	歐元區民眾檢視鈔票真偽造之頻率.....	18
圖 4-3-1	墨西哥印鈔廠原生產線配置.....	19
圖 4-3-2	墨西哥印鈔廠新廠房平面配置.....	21
圖 4-3-3	墨西哥印鈔廠新廠房規劃時程.....	22
圖 4-3-4	墨西哥印鈔廠新廠房 2016 及 2017 建置進度照片.....	22
圖 4-3-5	埃及現金需求成長預測.....	24
圖 4-3-6	埃及印鈔廠建造時間規劃.....	25
圖 4-3-7	埃及印鈔廠生產線內容規劃.....	26
圖 4-4-1	澳洲鈔券宣傳 app 畫面擷取.....	27
圖 4-4-2	泰國鈔券宣傳 app 畫面擷取.....	28
圖 4-5-1	愛沙尼亞 X-Road 架構圖.....	31
圖 4-5-2	2002 年至 2019 年愛沙尼亞 eID card 發行人數.....	32
圖 4-5-3	愛沙尼亞晶片身分證 (eID card).....	35
圖 4-6-1	區塊鏈去中心化系統.....	47

圖 4-6-2	區塊鏈之應用範圍	48
圖 4-6-3	區塊鏈集中和分散系統概念圖	49
圖 4-6-4	簡單的區塊鏈交易流程	50
圖 4-7-1	馬爾他國民身份證 (National ID) 之發行歷史	54
圖 4-7-2	馬爾他國民身份證正面之防偽特徵	56
圖 4-7-3	紫外線 (UV) 光下之馬爾他身份證	57
圖 4-7-4	馬爾他國民身份證背面之防偽特徵	57
圖 4-7-5	馬爾他晶片護照正面之防偽特徵	58
圖 4-7-6	馬爾他晶片護照背面之防偽特徵	59
圖 4-7-7	馬爾他晶片護照簽證內頁之防偽特徵	60
圖 4-8-1	ISO14298 認證	62
圖 4-8-2	CWA 15374 認證	63
圖 4-8-3	INTERGRAF 認證效益圖	64
圖 4-8-4	《INTERGRAF 認證要求 (ICR)》細節	66
圖 4-8-5	INTERGRAF 認證週期圖	67
圖 4-8-6	De La Rue 總部和其他現場通過 ISO 14298 之時間表	70
圖 4-8-7	全球 INTERGRAF 認證概覽	71

表 目 次

表 3-1	2019 年國際安全印刷人會議 (SecurityPrinters) 議程表	5
表 4-2-1	CE 版巴哈馬鈔券使用之安全特徵規劃	13
表 4-3-1	墨西哥印鈔廠方案評估	20
表 4-5-1	破解不同複雜性 RSA 金鑰所需時間與成本.....	39
表 4-5-2	愛沙尼亞數位身份證 ROCA 危機處理時間軸	49
表 4-6-1	集中投票與分散投票比較表	51
表 4-6-2	選舉中的各利益相關者	51
表 4-8-1	ISO 14298 認證費用明細表	68
表 4-8-2	CWA 15374 認證費用明細表.....	69
表 4-8-3	De La Rue 通過認證之分公司	70
表 4-8-4	全世界取得 ISO 14298 及 CWA 15374 認證之等級及公司家數	71
表 4-8-5	全世界取得 ISO 14298 及 CWA 15374 認證之國家與公司家數	72
表 4-8-6	台灣取得 ISO 14298 認證之公司	73

壹、前言

本次國際安全印刷人會議（SecurityPrinters）由位於比利時布魯塞爾的 INTERGRAF 協會舉辦。1930 年成立的 INTERGRAF，自 1976 年在義大利米蘭針對鈔券（Banknotes）及身分文件（Identity）舉辦第一次的國際安全印刷人會議後，每 18 個月會選定一歐洲城市舉辦，至今已超過 40 年，為安全印刷相關產業之重要盛會。

本次 2019 年國際安全印刷人會議，相隔 4 年後又再次回到哥本哈根舉辦，召集鈔券與身分文件之發行機構、政府機關、安全印刷業者及供應商，共同了解當前產業現況，並對未來的發展與需要提供願景，例如對於考慮鈔票、護照或身分證改版的發行機構或政府機關，正可藉此平臺與提供解決方案之業者，探討如何開發與改進新技術，從而使安全印刷品的使用壽命更長，更易於管理及使用。

本屆會議主軸是「身分和金錢的未來（The many Futures of Identity and Money）」由未來學者 Rohit Talwar 進行開幕主題演說，接下來的議程包括 AR 擴增實境、鈔券與身分文件之防偽功能及偽造趨勢等重點，而會議最後一天的小組討論，來自法國央行、英格蘭銀行和丹麥國家銀行的高層代表，以及克銳貨幣總裁與 G+D Currency 之 CEO 組成小組討論「變更所有權結構對鈔券供應鏈之影響」。此外，本屆還有一個慶祝活動：瑞士安全印刷廠商 OrellFüssli 發表從文藝復興 500 年之紀念鈔。

貳、目的

一、拓展視野

參與國際會議是一個拓展視野及增長知識的好機會，國際安全印刷人會議（SecurityPrinters）將來自世界各國安全印刷產業相關業者及供應商聚集在一起，互相結識、建立聯繫、彼此學習、分享經驗，有助於開拓視野。特別的是，此會議聚焦在鈔券（Banknotes）及身分文件（Identity），且開放對象僅限於安全印刷業者、安全印刷供應商、鈔券發行機關、政府機關、執法機構及郵政機關等，因此探討內容更為深入，參與者可以有更好的學習效果。

二、與國際接軌，掌握先機

各種科技日新月異，安全印刷產業科技亦是。本廠為國家級印鈔廠，承製我國鈔券及身分證、護照及各式有價證券等安全文件，當應與國際接軌，不斷掌握安全印刷產業之新科技、新觀念與新趨勢，以對抗因科技進步而日益增加之偽造案件。本次會議有許多演講者分享仿冒身份文件之最新發展和趨勢、數位印刷科技對仿冒品之影響，以及鑑識仿冒品之實際案例，有助於本廠未來設計有價證券時，可預先避免被偽造之機會。

三、他山之石可以攻錯

國際安全印刷人會議邀請之演講者皆為安全印刷產業界之專家，依據他們的專業知識提供務實的見解及真實的經驗，議題包括近年鈔券改版、建置新廠房經驗、仿冒文件鑑識、仿冒文件趨勢、身份認證、區塊鏈應用、安全文件材料演進、愛沙尼亞 eID card 資安漏洞及 ISO/CWA 認證等。正所謂他山之石可以攻錯，本廠正值轉型之際，相信他國經驗對於未來在鈔券改版、新廠房建置或新業務承攬時，可以提供更多啟發以避免錯誤，減少耗費時間及降低無謂成本。

叁、會議過程

一、會議簡介

(一) INTERGRAF 協會

INTERGRAF 之全名為 International Confederation for Printing and Allied Industries – INTERGRAF，1923 年於瑞典之 Göteborg 起草籌備，1930 年於德國柏林正式成立，初期名稱訂為「國際主要印製者聯盟」(International Bureau of the Federations of Master Printers)，1946 年曾遷英國倫敦，後又遷至現址比利時布魯塞爾。INTERGRAF 係由歐洲地區相關行業之成員組織而成，其主要工作及業務範圍包括歐洲印刷相關工業政策之制定，同時代表木材業、造紙業及紙漿供應用等行業代表為業者發聲，並維護其權益。

INTERGRAF 為專門從事安全印刷研究之非營利組織，目前擁有來自歐洲 20 多個國家之會員，以促進和保護安全印刷產業之利益，並通過推廣、提供信息和建立網絡來支援安全印刷產業，並提升其競爭力，為競爭日益激烈的挑戰提供解決方案，主要任務包括：

- 為安全印刷廠商、供應商及客戶提供互動平臺。
- 在國際上代表安全印刷行業之利益。
- 討論新技術、新興市場、打擊假冒偽造產品，以及任何其他與安全印刷業有關之主題。
- 積極推廣 ISO 14298 與 CWA 15374 認證，以促進和保護安全印刷業者及供應商之利益。
- 定期發行《Infosecura》季刊，為安全印刷產業提供技術和產品發展之相關報導。
- 定期舉辦國際安全印刷人會議 (SecurityPrinters)，為安全印刷相關產業建立交流平台。



圖 3-1 本次會議地點 Bella Center Copenhagen

（二）國際安全印刷人會議（SecurityPrinters）

在 1976 年第一屆國際安全印製者會議於在米蘭召開時與會代表人數不多，但現已成為全球討論文件安全印刷防偽最重要之年度盛會之一，每隔一年半舉行一次，選定一歐洲城市舉行，邀請所有中央銀行、安全印刷相關從業人員、設備廠商、鑑識人員、國際/各國刑警、海關人員等，就鈔券及身份證明文件之印製發行、使用流通、辨認鑑識等領域的各種最新發展趨勢動態進行交流，以對抗隨科技發展而日亦增加的偽造案件。

相較於其他會議，國際安全印刷人會議（SecurityPrinters）特色包括：

1. 會議聚焦在鈔券（Banknotes）及身分文件（Identity），因此探討內容更為深入，參與者可以有更好的學習效果。
2. 僅向安全印刷業者、安全印刷供應商、鈔券發行機關、政府機關、執法機構及郵政機關開放，所有參與者皆須向 Intergraf 的專家委員會提交詳細個人檔案及其公司產品樣本，經該委員會評估其資格後，始可參與會議，若不符合要求條件，Intergraf 則保留拒絕參加的權利。
3. 邀請之演講者皆為安全印刷產業界之專家，根據他們的專業知識提供務實的見解及真實的經驗，以解決當今產業面臨之難題。
4. 國際安全印刷人會議如同一個平臺，將安全印刷產業相關業者及供應

商結合起來，建立新聯繫並形成網絡，建立富有成效的合作夥伴關係。

二、會議議程

本屆 2019 年國際安全印刷人會議（SecurityPrinters）自 2019 年 10 月 22 日至 25 日於丹麥哥本哈根的 Bella Center 舉辦，主題包括防偽科技、防偽設計、防偽鑑識、偽造趨勢及邊境管理等，會議分為三大部分：

- （一）鈔券及身分證明文件高階安全印刷人會議（Banknote/Identity High Meeting），共 20 場演講。
- （二）鈔券及身分證明文件安全印刷人研討會（Banknote/Identity Conference），共分為 12 個主題，42 場演講。
- （三）展覽（Exhibition），由將近 100 家世界知名廠商參展，展示最新技術及產品。

表 3-1 2019 年國際安全印刷人會議（SecurityPrinters）議程表

日期	議程
10 月 22 日	鈔券及身分證明文件高階安全印刷人會議 （Banknote/Identity High Meeting）
10 月 23 日	1. 鈔券及身分證明文件安全印刷人研討會 （Banknote/Identity Conference） 2. 安全印刷供應商展覽（Exhibition）
10 月 24 日	
10 月 25 日	

本次國際安全印刷人會議（SecurityPrinters）共有來自世界各國 900 多位參與者、70 多位演講者，以及 90 家世界知名供應商參展，藉此平臺聯繫交流並獲取新知。

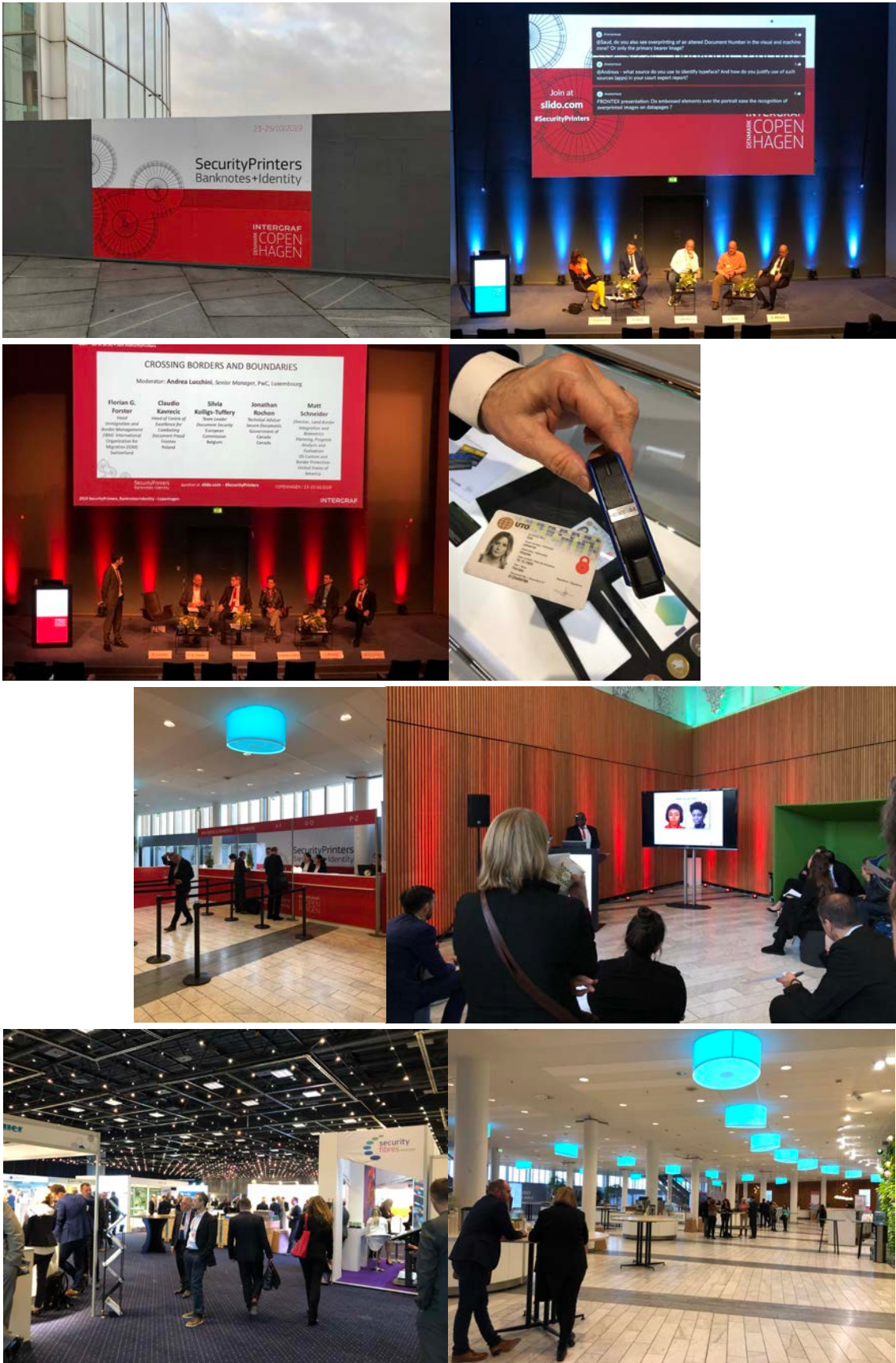


圖 3-2 會場集錦

肆、會議內容

一、身分和金錢的未來

本屆會議主軸是「身分和金錢的未來 (The many Futures of Identity and Money)」，由倫敦智庫「快速未來研究 (Fast Future Research)」之 CEO Rohit Talwar 發表開幕主題演講，他是一位全球未來學家、演講者、作家和戰略家，幫助企業適應不斷變化的全球經濟的需要，提供金融、工業和科技等趨勢，協助企業在動盪時期將風險轉為機遇，創造最佳績效，從而提高其競爭地位。他的客戶包括英國廣播公司 (BBC)、諾基亞 (Nokia)、松下 (Panasonic)、IBM、瑪律克斯 (Marks) 和斯賓塞 (Spencer) 等，並發行過許多暢銷書。

他指出，在一些國家，非現金支付呈上升趨勢，現金支付比率在下降，關於現金的未來及何時可能被邊緣化，甚至消失，有好幾種預測。對一個未來學家來說，無現金社會的問題將呈現出許多有趣的情景，例如，中央銀行將貨幣政策轉讓給少數國際信用卡公司，限制了數百萬人旅行的能力，因為他們無法使用信用卡或手機。任何政府都不太可能以剝奪其部分公民權的方式，而放棄貨幣政策，這些暗示聽起來像是危言聳聽，但無論誰被賦予發行貨幣的權利，都必須證明貨幣對所有人都是可接受的。

作為未來學家的角色是探索影響未來的許多力量和因素，並考慮不可預見的可能性。金錢和身份對於人類的生存至關重要，涉及許多經濟，政治，社會，法律，技術甚至環境方面的因素，必須在未來可能出現的情況下處理這些問題，然後應對可能出現的機遇和挑戰。

身份和金錢是 21 世紀生活的基石，而數位化正在改變兩者的概念，一方面，區塊鏈 (blockchain) 和人工智慧 (AI) 等科技使身份和金錢都可以因為數位化，並從被動對象轉變為可程式設計的代幣；另一方面，感測器、邊緣計算 (edge computing) 和生物識別技術 (biometrics) 能夠將數位化功能轉移到實體領域，從而為護照、金錢和以前具有單一功能的物體帶來潛在的新生命。再往

前看，腦紋（brainprinting）、生物學、DNA 存儲和生物學計算方面的突破，為我們如何管理身份，存儲金融資產和進行價值交換開闢了全新的可能性。

在短期內，我們可以想像各國發行的數字貨幣激增，我們還可以想像代幣化模型，其中現金，商店忠誠度積分，甚至社交媒體的「讚（like）」都可以被視為生態系統中可互換的支付機制，亞馬遜明天就可以這樣做。從長遠來看，一種單一的全球數位貨幣可能會出現。

這同樣適用於實際身份證件，一些國家正在採取長期措施，以取消實體駕駛執照，身份證和護照，憑藉先進的面部識別技術，一些旅行者現在或未來幾年都可能在無需出示任何身份證件的情況下進入機場並登機，在民主國家真有可能有一個沒有實際身份證的身份證系統嗎？這與民主無關，無論身在何處，都需要各種形式的身份證。業界可以嘗試防止這種情況發生，但趨勢正轉向採用生物識別技術來保護存儲在區塊鏈上的數位識別碼，各國政府認為這在保護身份、提高效率、減少紙張及減少欺詐風險等方面有好處。

從這些問題中還引出其他幾個問題：抵制這些潛在的變化，應該採取什麼行動？什麼是強化和提升傳統解決方案的優勢？如何尋找將物理和虛擬結合起來的方法？還有其他選擇嗎？Rohit Talwar 說，如果他是這個行業的領導者，將會研究影響未來 5-15 年的因素，並提出下列戰略方案為明天的世界做準備，值得我們深思：

- 在數位世界中，金錢和身份的某種未來似乎可能是什麼？
- 會出現哪些機會來增強和調整印刷有形資產的用途？
- 在新的萬億美元（\$Tn）行業中，我們可能將出現何種可能性？
- 我們應該如何以及在何處投資於人員，技術和新業務，以便為接下來的幾項戰略行動提供一個健康的選擇組合？

二、鈔券改版跟設計

(一) 香港鈔券改版

在 2010~2018 年期間，隨著到訪香港遊客數的增加（2018 年遊客數為 6 千 8 百萬人次）以及 GDP 成長，港幣在現金各面額的需求不管是在數量或是總面額的部分均穩定成長(圖 4-2-1)，故其為了(1)領先偽造者一步—使用最新的防偽科技，(2)增加鈔券使用壽命—新鈔券採用印後上光，使流通券更佳清潔並可增加耐用度，(3)將防偽特徵以及設計主題制定標準，方便民眾以及機器辨識，(4)維持民眾對港元及金融穩定的信心等上述原因，依計畫陸續發行新版港幣鈔券。目前發行的有：2018 年 7 月發行的面額 1000 元、11 月發行的面額 500 元以及 2019 年 9 月發行的面額 100 元，並計畫於 2020 年 1 月發行面額 50 及 20 之鈔券。

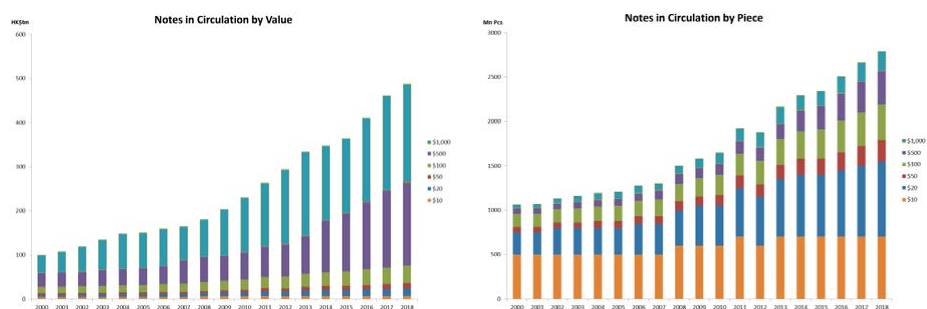


圖 4-2-1 2000~2018 年港幣各面額票面總額(左)及各面額流通張數(右)變化
(資料來源：2019 Intergraf Copenhagen proceedings)

因港幣同時由三家銀行發行，故本次改版先規畫其安全性特徵並規劃出其版面配置（圖 4-2-2），其所使用之安全性特徵有：

1. 正反套
2. 折光變色效果(SPARK® LIVE)
3. 面額採凹凸手感
4. 面額隱藏字
5. 窗式安全線

6. 珠光墨
7. 微量元素 (SICPATALK®)
8. 直/橫式併陳打碼

並指定相同面額均須使用相同之主題及顏色，制定五個面額分別展示香港的金融中心、地質公園、粵劇、蝴蝶、茶點。再交由各銀行及其設計印刷單位來規畫。其原因除方便機器閱讀外，也可縮短民眾認識鈔券及辨識面額之時間。

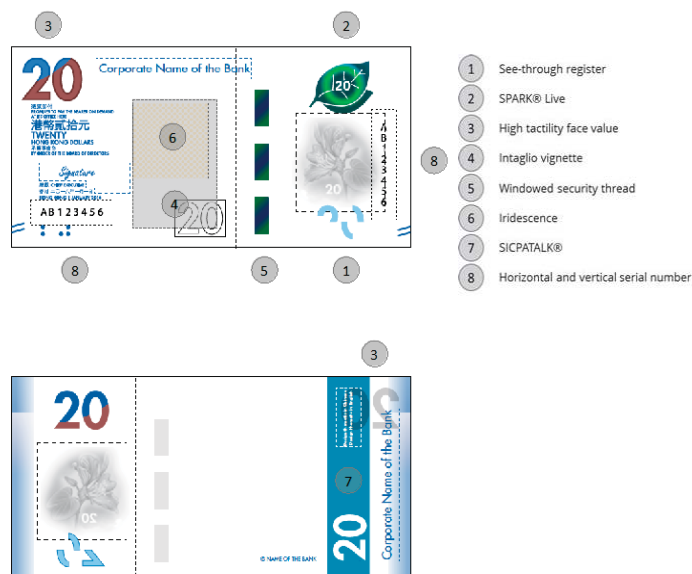


圖 4-2-2 新版港幣正、背面之功能性規畫
 (資料來源：2019 Intergraf Copenhagen proceedings)



圖 4-2-3 不同銀行所發行之新版一千元港幣

而在輔助識別的功能部份，除了使用常見的點字、手感線以及鈔券面額採凹版印刷等規畫，可供視障人士辨別外，其配合專門研發之手機 App—讀鈔易(HK \$ reader)，可在 App Store 和 Google Play Store 免費下載。該軟體透過智慧型手機的相機擷取鈔券影像以辨識出面額，並發出語音讀出港幣的面額，同時提供震動功能，分別以一至三下短促之震動來表示 10 元、20 元、50 元；一至三下較長之震動表示 100 元、500 元、1000 元。在語言支援方面，操作介面提供中文及英文兩種可切換，而朗讀面額語音的部分，亦為不同母語居民提供普通話和廣東話。但此 App 僅能區分面額而無辨識真偽功能。



圖 4-2-4 協助視障人士辨識港幣面額之 App—讀鈔易使用畫面
(圖片來源：App store)

(二) 巴哈馬 CRISP Evolution 系列鈔票

經過近三年的規劃和開發，巴哈馬中央銀行於幾週前將其 CRISP Evolution（後簡稱 CE）發行 50 元鈔券。這代表了業界首次將 Landquart 的 Durasafe 基材和 Crane 的 Rapid®整合在同一版面。接下來的發行計畫是在 2021 年在 Durasafe 發行的面額為 100 元的紙幣，其中包含了 Crane 的 Motion Surface™ 安全線，這是另一項業界首次整合此二種功能在一面額中。這兩種面額鈔券均由加拿大銀行印製。若其如預期能成功增加耐流通性，則將來會將其他棉紙印製的棉額亦轉用 Durasafe 以及混合式 Hybrid 來印製。

CRISP Evolution 系列背後所採用的策略共考慮四大面向：

設計 (Design) 每十年改版換新設計，每五年印一次，故共發行兩次。

安全 (Security) — 推廣現代，強大的安全功能，減少假冒的發生。

耐用 (Durability) — 結合更耐用的基材和功能，改善紙幣壽命。

易用 (Usability) — 人性化功能；簡單是關鍵，使視力障礙人士也更方便使用。

而該國此次改版自 2012 年起便開始規劃，其依上述考慮的四個面向來做評估：

設計 (Design) — 設計是否仍然有意義且最佳化？

否；自 2005 年以來發行/未引起共鳴，需要簡化和凝聚，使其更有效地被利用

安全 (Security) — 該系列是否具有最新最強大之防偽功能？

否；過時且非最強大的功能。每個面額均使用相似的功能，包括相似的圖紋，且時有一些偽造事件發生。

耐用 (Durability) — 若改用其他基材，使用壽命可以再增加嗎？

是；其使用壽命可從 11 到 29 個月不等，並可改用使用壽命更長之複合基材

易用 (Usability) — 此系列是否容易辨識？

否；鈔券特徵並不包含以下友善視障者功能辨識功能—面額符號小且在交易時難以區分，尤其是昏暗燈光下。

故其解決方案為將新版鈔券設計採用現代化和簡化設計—OrellFüssli 於 2013 年加入此一改版計畫，導入尖端技術，優化鈔券使用經驗並改善文化相關性/共鳴。此次改版著重下列各項：

材質—用於增強設計增加耐用 考量安全 防止各種程度的偽造。

安全線—使用壽命長的且具安全性的安全線，並使其搭配最佳化設計。

視力障礙者的使用—與當地弱視群體接觸討論，添加方便視力障礙者使用的符號及功能使其容易區分各面額，使鈔票不單僅為多數人，而是為了所有國人所設計及使用。

表 4-2-1 CE 版巴哈馬鈔券使用之安全特徵規劃

面額	實用功能	鈔券基材	安全線
\$½和\$3	使用度低	棉紙	STARSheen™
\$1 和\$5	低面額	複合性材質(Hybrid™)	Rolling Star®
\$10 和\$20	交易	經塗佈之棉紙	Active™
\$50	儲蓄	複合性材質(Durasafe®)	Rapid®並使用磁性油墨
\$100	儲蓄	複合性材質(Durasafe®)	Motion Surface®並使用磁性油墨

(資料來源：2019 Intergraf Copenhagen proceedings)

而目前已流通改版之鈔券面額及成果，在 2016 年發行的 10 元面額的部分，係採用塗佈之棉紙為基材，但其平均使用壽命僅由 12 個月提升為 15 個月，和前一版相較無統計上差異；而 2017 年發行的 1 元面額採用混和材質使用複合性材質(Hybrid™)，其使用壽命則由 13 個月提升至 22 個月。參考圖 4-2-5 可知其被偽造率從 2016 年後開始下降，在 2017 年雖有被偽造但是其品質粗糙低劣和真鈔品質出入極大，且在後被偽造之比率亦趨下降。

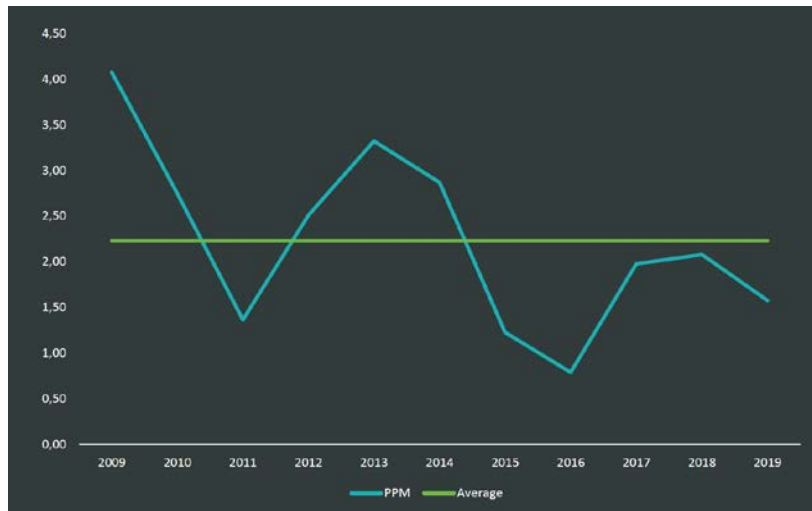


圖 4-2-5 巴哈馬近十年鈔券被偽造率
(資料來源： 2019 Intergraf Copenhagen proceedings)

而此系列尚有兩種面額待發行—預計在 2020 發行 CE \$5：採用複合性材質(Hybrid™)搭配使用 Rolling Star®安全線，以及在 2021 發行 CE \$100：印刷在 Durasafe®並搭配 Motion Surface®安全線。而先前發行之 CE \$10 原採取塗佈之棉紙印刷，鑒於其使用壽命並無顯著延長，故計畫於將來以和現有版本相同之印刷設計移至複合式紙張上印刷發行。此系列將來計畫將繼續提高安全性、耐用性以及易用性。並繼續保持開放的態度，依民眾回饋之使用經驗，繼續尋求進步且適當的可行性方案。

(三) 從 EUROPA 系列中汲取的經驗

歐元 EUROPA 系列於 2019 年 5 月 28 日分別發行了 100 歐元和 200 歐元面額之鈔券。並於 2017 年開始綜覽過去十幾年來其研發、生產、發行的經驗。從中汲取了一些重要的經驗教訓，其包括必須持續注意到所有相關產業需求的變化，和其引導開發工作的緊迫性，故在設計發行鈔券時不僅要考慮技術的進步，還要考慮市場的發展以及鈔票流通環境。

而透過這些檢視，得到一個重要的教訓是：開發適合目的的新鈔票需要花費大量時間。因此，鈔票發行機構應在鈔票發行前，就已著手在設計，在其中就加入的新功能並進行測試及改進，以便在適當之時機即開始生產新

版。這種時機可能是相關產業或是使用者需求的變化，政策決定更改一種或多種面額的設計，或更重要的是可能已經面臨被偽造的威脅。在沒有上述情況下，亦應考慮鈔券可能會有定期改版的中程計劃。

迄今為止，已將這次所回顧整理所學到的經驗，最大程度地運用於 EUROPA 系列最後一個面額的開發過程中。而這個研究將繼續進行，並將塑造未來紙幣發展的框架。而且也必須加入市場的最新發展評估，例如其他支付方式的出現和快速增長，亦需要進行徹底的分析以評估長期現金使用的演變。在可能的情況下，應加強其主要功能（例如便利性、可再回收、社會接受度、安全和保障，成本等），以強化現金成為與其他付款方式競爭力。

長期來看我們是否還需要鈔券？以 4-2-6 圖參考資料來看，近 10 年歐元的發行數量來看，其每年仍維持 4.5% 之年增率，而參考圖 4-2-7 可知，不論以交易筆數或是交易金額來看，絕大多數的歐元支付仍是透過現金支付的方式。

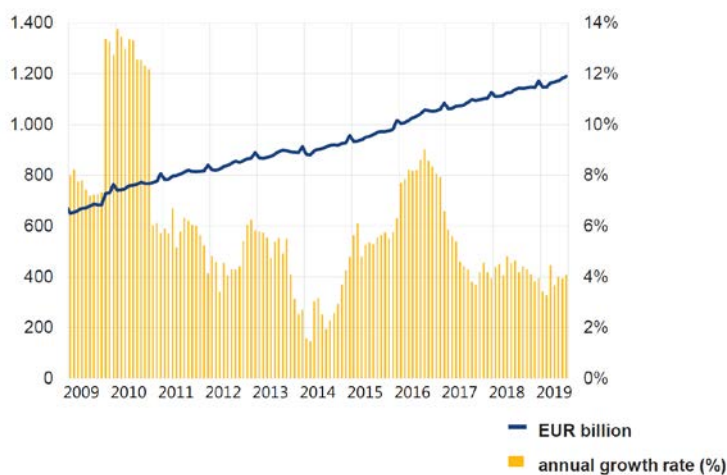


圖 4-2-6 歐元發行數量及年增率
(資料來源： 2019 Intergraf Copenhagen proceedings)

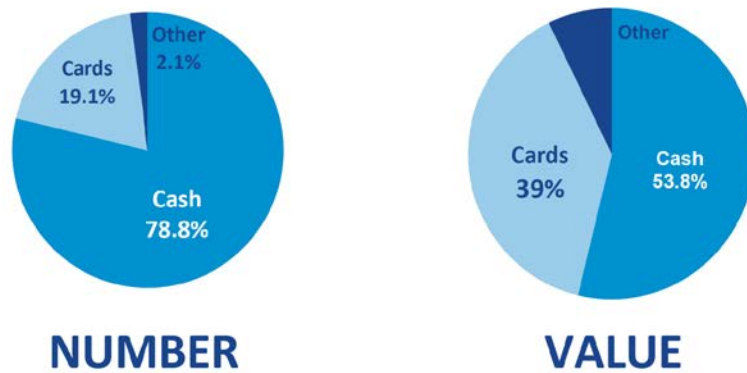


圖 4-2-7 歐元交易以筆數(左)及金額(右) 顯示之支付方式比率
(資料來源： 2019 Intergraf Copenhagen proceedings)

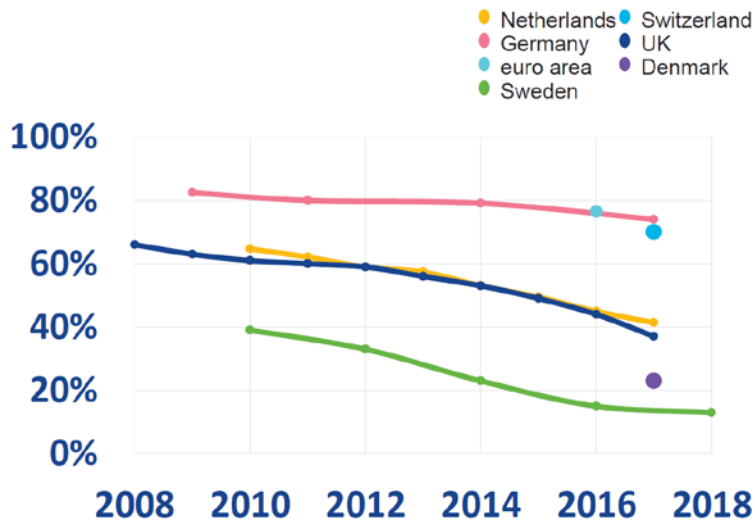


圖 4-2-8 歐洲各國銷售點交易的現金所占比率
(資料來源： 2019 Intergraf Copenhagen proceedings)

歐元紙幣流通量呈現強勁增長，根據統計調查，1/3 的歐元區公民喜歡現金支付勝於所有其他付款方式。然在此同時，比較歐洲其他各國銷售點交易的現金所占比率，看到現金的使用趨勢卻是下滑(圖 4-2-8)。甚至有一些研究預測到了 2030 年現金使用在某些國家會被邊緣化，預測在此同時，超過 50% 的歐元可能會轉而使用於 POS 機而非人工交易(以紙幣數量計)。縱然如此，在此同時歐元的發行仍需確保實體鈔券的可用性和可接受度予想要使用現金的人。

而以目前的檢視結果來看，現今發行的系列歐元(Europa Series)是否是個成功的商品？其是否符合現在的使用需求？經過歐洲央行(UFS)的調查研究品質良好（新紙幣和流通量），而在公眾的回饋亦是良好的，其有高度的信任度，此系列歐元的安生性亦維持相當高，且越來越多歐元區的人民對其產生正向喜好感情。

另外在零售點方面，越來越多交易導入使用機器來交易，而此版歐元相較第一版之歐元，不論 IR、UV 或是磁性油墨方面都更臻成熟，有些已可完全運用於之鈔券設備製造商(banknote equipment manufacturers,BEMs)。

在生產和流通的永續性面向，其使用壽命因為塗層的使用，使其使用壽命延長了約 40%（換算每年節省 8000 萬歐元）。故決定，從 2020 年開始面額 20 歐元也會加上塗佈的工序。為追求環境永續發展，基材使用部分目前的中程規劃仍會使用 100%可再回收利用或處理之棉紙而非使用複合式或是塑膠材質。

在生產成本方面，因原材料供應競爭加劇，故必須持續仔細監控其標準和實際生產成本；而在發行和循環成本，為了減少機器調整的成本，分組發行不同面額；另外，使用塗佈亦可延長紙幣的使用壽命。

在與相關產業的接軌方面，在 5 歐元的發行之初，因為準備不足亦不了解 BEMs 使用成長日趨重要，也不知道供其機器使用所需條件，故當時為預留 BEMs 的準備不足。有此經驗後，後續的歐元發行均會先提早約九個月提供樣張供 BEMs 建立合作，故現在新發行之歐元已無鈔券相關設備使用之問題，而新興市場國家現在對歐元體係採取的措施亦感到滿意。在大多數歐元地區，人民使用經驗回饋均是正面的。

關於新系列歐元宣導方面，75%的民眾認為其宣導做得相當的好，有接受到辨識防偽宣導教育，而在專職使用鈔券人員，例如負責收銀者，在此部分和一般人表現幾乎無異。但在此調查有一項令人意外的結果，針對鈔券的安全特徵，儘管大眾均有受到宣導教育，絕大多數的民眾在經手鈔券時並不

會去辨別其真偽，參考圖 4-2-9，僅有 7% 民眾每次會檢視鈔券真偽，17% 經常檢視，25% 偶爾辨識真偽，30% 民眾僅以很低的頻率會去辨識，而甚至有 21% 的人從不去檢視拿到的鈔券是真鈔或是偽鈔。其透漏幾個訊息，偽鈔率不高以及交易中用來辨識的方式已經轉委由機器閱讀辨識。故在將來設計發行新系列之歐元時亦需將此納入考量，是否還需要放入過多的安全防偽特徵？過多的特徵可能在設計或是印刷適性上均會互相干擾，亦會造成成本的增加，但是若過少的安全特徵亦可能造成鈔券容易被偽造，因此在其運用的數量上必須要取得平衡，另外亦要將機讀的重要性加成，故未來將針對零售業開展專門研究。隨著環保意識抬頭，環保議題在鈔券上越來越重要，其環境足跡和鈔券生命循環(回收或銷毀)均是關注的重點，但在此同時，許多數位支付方式如雨後春筍般出現，故在持續關注鈔券使用狀況外，亦需注意整個支付方式環境的變化，以做出因應。

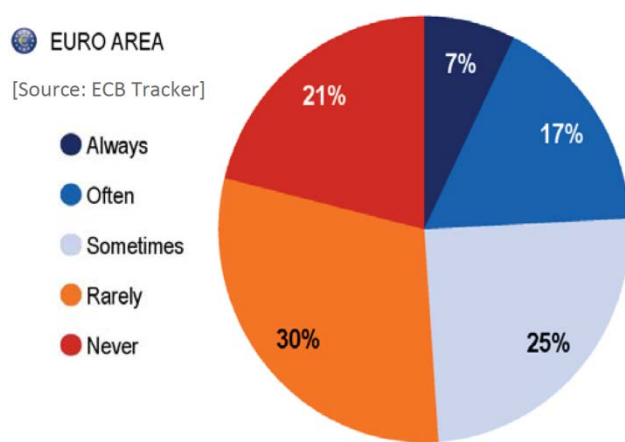


圖 4-2-9 歐元區民眾檢視鈔票真偽造之頻率
(資料來源： 2019 Intergraf Copenhagen proceedings)

三、建置新廠房

(一) 墨西哥

墨西哥銀行於 1969 年始在墨西哥城的印刷廠開始生產鈔票。多年來，印刷廠的利用率已達最大化。在 2010 年時，其機器配置有下列一

- 2 臺平凸印機 (Offset press)
- 1 臺網印機 (Screen press)
- 2 臺凹印機 (Intaglio press)
- 2 臺號章機 (Numbering press)
- 2 臺上光塗佈機 (Varnishing press)

其生產線配置如圖 4-3-1，其中網印機僅配置於當中一線係因為墨西哥鈔票並非每個面額都有採用 Spark®功能網印設計，故在評量需求後僅有一線有配置網印機。



圖 4-3-1 墨西哥印鈔廠原生產線配置
(資料來源： 2019 Intergraf Copenhagen proceedings)

但在 2010 年底鈔票使用需求的預測表示，在未來幾年的生產需求將超過預期，目前之產線已不足以應付，故墨西哥貨幣發行總局分析了五種提高生產能力的不同解決方案來評估，並依其安全性及成本作為主要考量點(表 4-3-1)。最後選定的結果是在該國另一個城市建造另一個印刷廠。當方案選定後，理事會便派出一個顧問來驗證墨西哥銀行在 2012 年進行的分析。主要結論是該項目有其充分必要性的，並且選定瓜達拉哈拉 (Guadalajara) 為新廠最適合的座落城市。

在選定方案後，從 2013 年 4 月到 2014 年 10 月這段期間，找尋各個廠商進行諮詢，目的是開發和實施以下項目：

1. 建築和設施工程的建築設計
2. 印刷設備選擇
3. 建築物的安全性規劃。

諮詢結束後，統整蒐集的資料並進行市場研究以選擇一家建築公司。其過程只邀請符合設定標準的公司參加，然後從中選擇提供最優惠價格的公司委託營建任務。該項目為兩年期計畫，於 2015 年 10 月開始施工建造廠房。

表 4-3-1 墨西哥印鈔廠方案評估

方案	花費	風險
實施更多輪班	\$	●
搬遷至墨西哥市他處並安裝第三線生產線	\$\$\$	●
在目前印刷廠安裝第三線生產線	\$\$\$	●
進口鈔券	\$\$	●
建立新的分廠	\$\$\$\$	●

(資料來源： 2019 Intergraf Copenhagen proceedings)

在進行諮詢的同時，同時亦確定了項目涉及的每個領域的負責人，例如建築，IT，安全性，此外，還要求提出每一單獨預算以評估項目的總成本。這導致該廠遇到了最早的問題之一：由於有一分責單位並不是貨幣發行相關單位，對此預算項目不感興趣，因此不願花時間和精力為他們認為從未見過的項目擬定預算，從而導致估算錯誤和計算錯誤。

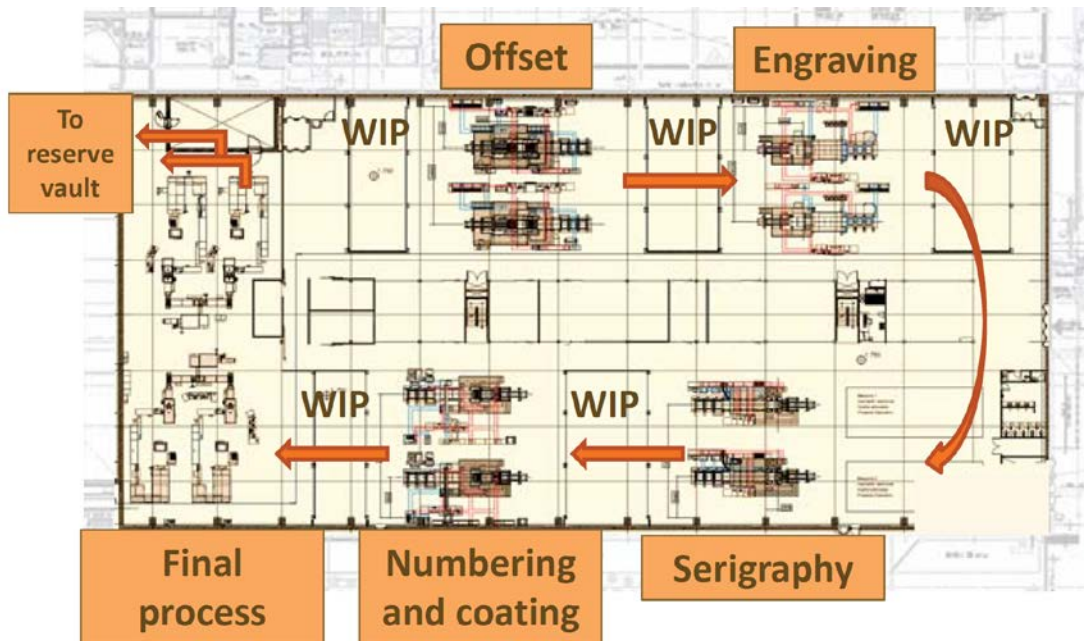


圖 4-3-2 墨西哥印鈔廠新廠房平面配置
(資料來源： 2019 Intergraf Copenhagen proceedings)

最終使用的樓面生產線配置採用簡化的 U 型設計，其使生產流程動線簡單化，之間直接存放半成品，故此工作動線不需再進庫房領料處理。存放拿取備品亦更方便。

而設備選擇方面，其研究的方法針對主要設備的市場研究，包括：印前設備、印刷機、檢查系統、儲存系統，油墨生產線等。而實際測試的方式則為使用墨西哥現行設計和材料在各種印刷機、印碼機等機器上進行實際之生產測試。在開發建築設計時，各項主要設備均未完全決定，因此，我們沒有工程計劃所需的資訊可供參考，因此創建了特殊的解決方案—將廠房空間暨高度均預留。

原始時間表規劃該建築利用兩年期間建設，於 2017 年夏季完工，因此印刷設備的安裝可以在 2017 年下半年完成，並於隔年(2018 年)1 月可開始投入生產。儘管如此，由於執行人員的一些錯誤，項目時間表出現了一些廠房基本設備和安裝服務採購的延遲。這導致了巨大的挑戰—因為機器如期購買沒有延遲，這意味著該印刷生產線已準備在 2017 年 8 月安裝，並且人員已經開始

將其遷移到瓜達拉哈拉，但是新站點尚未準備就緒，所需的水電均尚未設置完成，新設備即使入廠亦無法安裝使用。

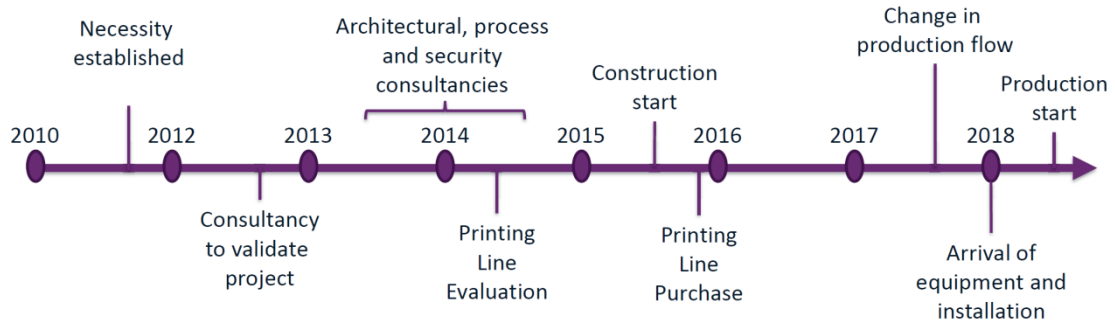


圖 4-3-3 墨西哥印鈔廠新廠房規劃時程
(資料來源： 2019 Intergraf Copenhagen proceedings)

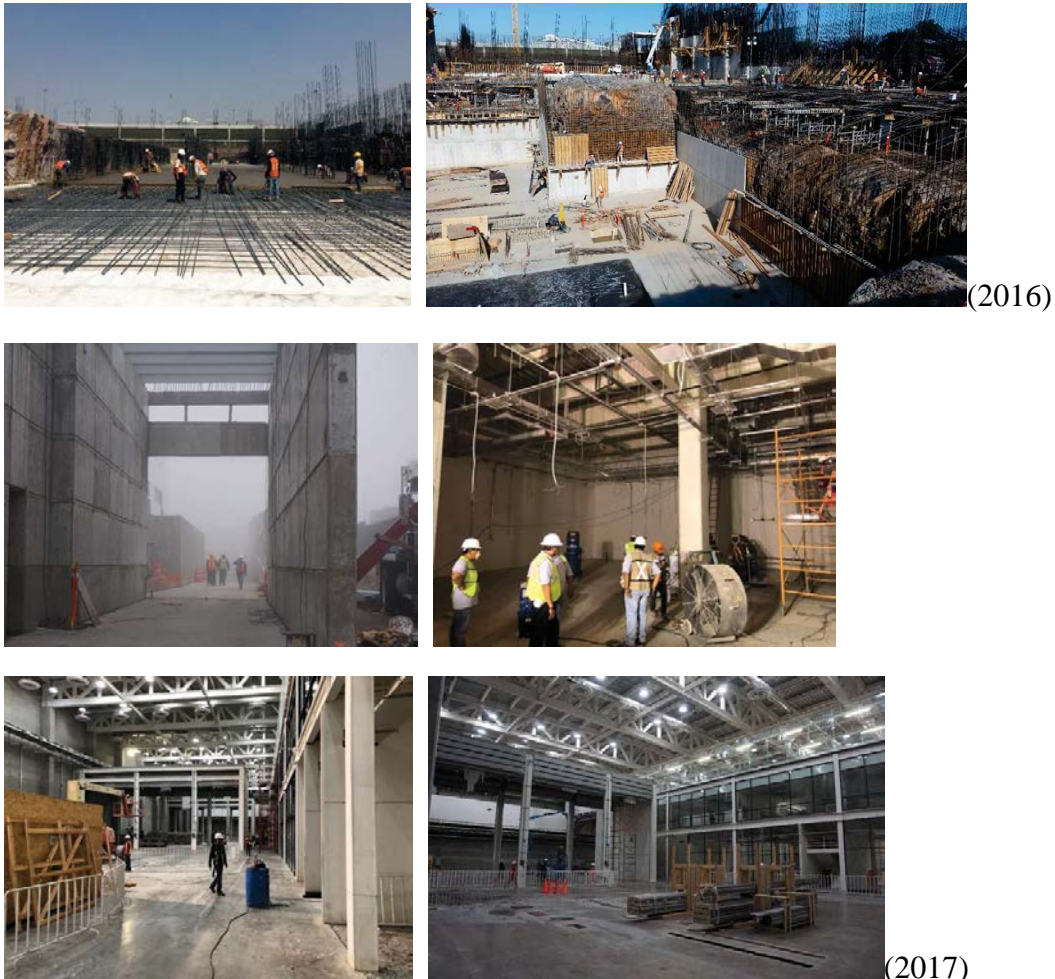


圖 4-3-4 墨西哥印鈔廠新廠房 2016 及 2017 建置進度照片
(資料來源： 2019 Intergraf Copenhagen proceedings)

在 2018 年上半年，儘管施工仍在進行中，但印前部門和主要印刷車間被隔離以防止灰塵進入，因此 CToP 和平凸印機的安裝僅能延至於 2018 年 1 月開始。而在機器安裝過程中，因為採購問題導致水電安裝延誤，故啟動了應急計劃，以便可以在計劃的日期進行生產測試。在新站點的建置過程中，正好在決定要進行一系列墨西哥紙幣的改版，從而也對生產流程進行了修改。當時印刷車間已經建成，甚至機器的設定也已經調校完成。對此需要機器供應商的支援以對新生產線的機器進行全面重新調整設定。最終生產於 2018 年 6 月成功啟動。以下是在此過程中獲得的一些經驗教訓：

- 明確定義項目的目標和範圍，使每個參與其中的人都能朝著同一個方向努力。一個項目必須有充分的信心和高度的認同這個規模以及如何進行。
- 在計劃階段，聽取其他印刷廠和中央銀行經驗建議，尤其是在樓面規劃的部份，應徵詢使用頻率最高的現場操作者意見，可以將規劃做得更好。
- 在開始施工之前，建議建廠規畫小組能包括不同專業的顧問。為了能確實執行規畫項目，應該在文件審查方面投注大量時間和相關人員來審閱設計文檔。在此階段進行更改或許可能會增加成本和時間，但如果是在後期階段（例如施工後）進行變更，則對成本和時間推遲影響會更大。
- 身為中央銀行單位，工程必須有透明度。故僱用了第三方來概括統包所有購買程序，以確保經濟資源使用的效率和透明度。
- 而在管理職責和簡化流程方面，建議將此一規模龐大的工程由一家關鍵廠商總包主責，因為與多個供應商合作會產生不兼容性，並且較難以協調。
- 明確定義溝通渠道並指定每個區域的負責人非常重要，在我們的案例中，運用 SharePoint 合併所有負責人的資訊帶來非常大的幫助。

(二) 埃及印鈔廠及整鈔中心

隨著埃及人口的穩定增長以及流通鈔券的數量穩定增長，可預測出的是埃及現有的、老舊的基礎設施以及印鈔設備均需要進行更新才能為將來做好準備，如圖 4-3-5 可見，在 2020/2021 年起，埃及對於現金的需求幾乎為過去的兩倍，作為中央銀行的角色必須確保鈔券的供應能在及時供應足夠的數量於需求市場流通，故 2016 年埃及中央銀行決心必須對此做出因應。

經過與相關行業專家一起進行的詳細分析，大家對如何進行這種轉變有了清晰的認識—為埃及中央銀行建立新的印刷廠和中央整鈔中心，以當作埃及新鈔券循環運作的基礎。

Forecasting of Growing Cash Demand in CBE

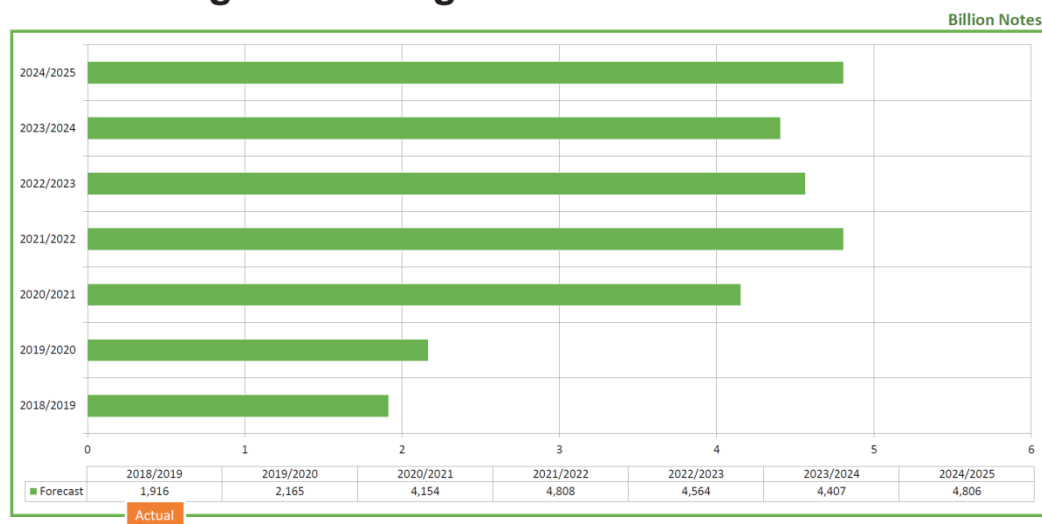


圖 4-3-5 埃及現金需求成長預測
(資料來源：2019 Intergraf Copenhagen proceedings)

埃及中央銀行決定從鈔券印製產業中尋求專業合作夥伴，以計劃和建設新的基礎設施，完成印刷和處理埃及的所有貨幣需求。這些新設施預計將於 2020 年建成並投入運營。通過使用最新技術和智能自動化，它們將提高現金循環流程的效率和安全性。此計劃中的另一個重要步驟是現有基礎架構的升級和連結。將使用新設備升級現有的三個現金中心，並在將來開設一個新的

區域現金中心。所有設施將以數位方式連接。這不僅可以更好地監控鈔票的流量更增強了預測功能，可以更有效地計劃生產和分配。透過導入尖端的 IT 和安全系統，以使這種數位化轉型成為可能，並保護所有關鍵基礎設施。

而在此一規劃及興建過程中，埃及的經驗建議為必須選擇合適的合作夥伴。由於這一興建及設備更新案的項目具有高度複雜度，必須考量所需的設備配置和技術需求、配置廠房及工作流程、印刷廠及現金中心的實體環境及數位的安全需求等，並且必須精確計算出成本以及時間流程，故選擇一個具有關鍵技術且可信賴的合作夥伴能夠確保此一專案在軌道上如期進行。

Project Time Schedule

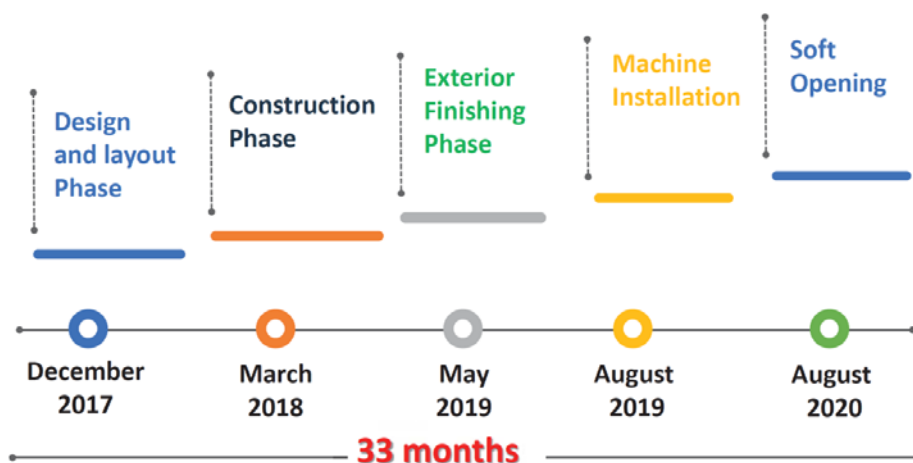


圖 4-3-6 埃及印鈔廠建造時間規劃

(資料來源： 2019 Intergrf Copenhagen proceedings)

如上圖所示，此建造案從設計至開始運作規劃於 33 個月內完成，根據規畫內容，會建置四條擁有最新技術水平鈔券生產線，每年最多可生產 48 億張鈔票的能力（以一天 24 小時/一周 7 天運作來計算）。其設備配置如圖 4-3-7，擁有最先進的設備，完全用軟體介面控制其生產，並均會連接到到 ERP 系統。可說擁有了最先進的實體和數位安全性。而為了確保初期能夠順利生產，機器等都搭配了五年的保固合約，其中三年採取全保固(包括零件耗材等)，使其機器效益調校為最佳化，發揮最大產能。其運作採用線上自動檢測系統，除可控制印刷品質，另外機上也搭配計數裝置，可對印刷數量及成品數量做一

追蹤，確保印刷過程不會有遺失的半成品。可控制質量控制與安全。另外在監控方面也以全面的監視系統（CCTV）以及採用數位管理的人出管制，取代過去以人工監視管理的方式以達最大程度的安全性。

此一印刷廠房更新，不僅只在硬體設備上，也會對從業員工進行一系列完整的授課訓練，規劃對維修技術人員實施最新技術的教育訓練共 2,200 人-工作天，印刷操作人員實施的教育訓練為 2,200 人-工作天。在本計畫完成後，能提供的產量及容量都將會是非洲-中東地區最大的。

New Printing House – High Automation, State of the Art Security

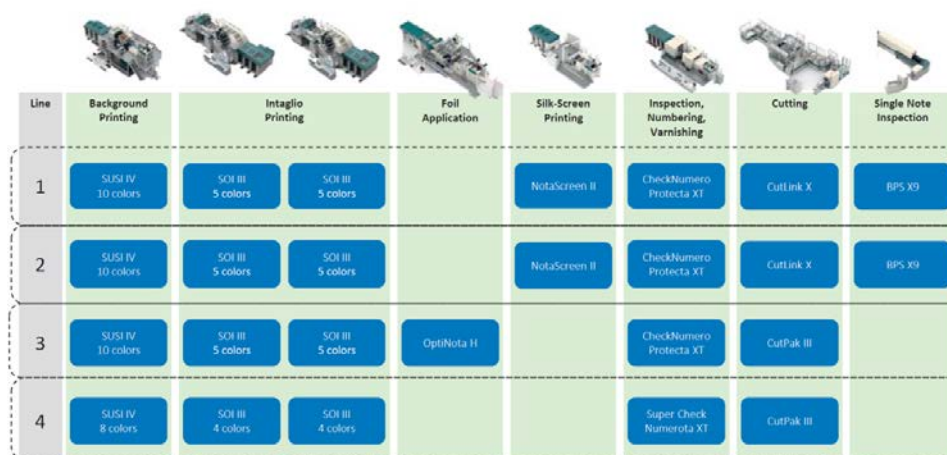


圖 4-3-7 埃及印鈔廠生產線內容規劃
(資料來源：2019 Intergf Copenhagen proceedings)

四、科技應用－將手機運用於鈔券推廣

透過報紙和電視接觸到傳播目標對象的時代已經結束。如今，幾乎所有人均是透過智慧型手機當作交流和獲取資訊的數位媒體。目前全球有約 77 億人，但手機有 51 億台，而社群媒體網站使用亦有 35 億個。所以在考慮鈔券宣傳時，已經不能只運用傳統的電視廣告和報紙等宣傳品，越來越多國家會在觸及率日益提高的手機開發 app。

澳洲日前釋出的 app 有針對鈔券的設計元素以及安全特徵透過互動之方式做簡短說明，亦可在 app 上觀賞辨識宣導影片。app 內提供鏈接到中央銀行的主頁，亦指引民眾在辨識後如拿到偽鈔或是破損的鈔券時需如何處理。但其在該 app 上架時選取鎖定於澳洲方能下載，無法提供不在澳洲境內的潛在澳幣使用者使用此一學習澳幣辨識的利器。

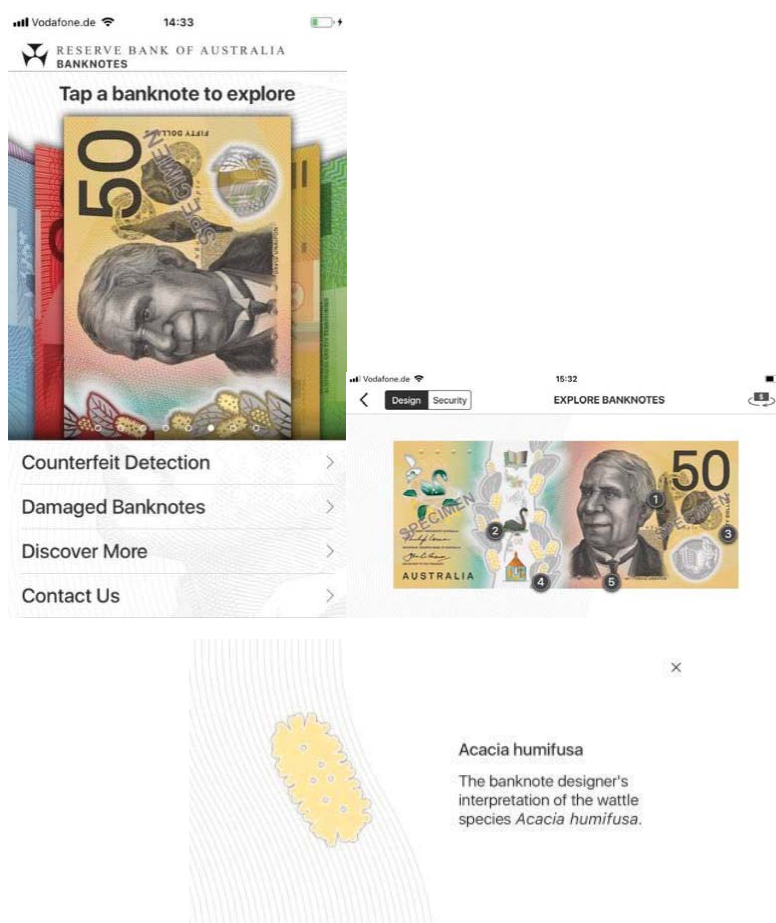


圖 4-4-1 澳洲鈔券宣傳 app 畫面擷取
(資料來源：2019 Intergrf Copenhagen proceedings)

而在泰國所製作的鈔券介紹 app 中，除對其內容及安全特徵利用文字描述，以針對其各個安全特徵互動按鈕來加深閱聽者印象，參考圖 4-4-2，該 app 在主頁面標示出全部安全特徵，但在選取每一單項時可切換到該安全特徵說明，並教導其辨識方法，或展示其在螢光燈下效果，另外其提供了語言切換的功能，方便外國人也能使用。

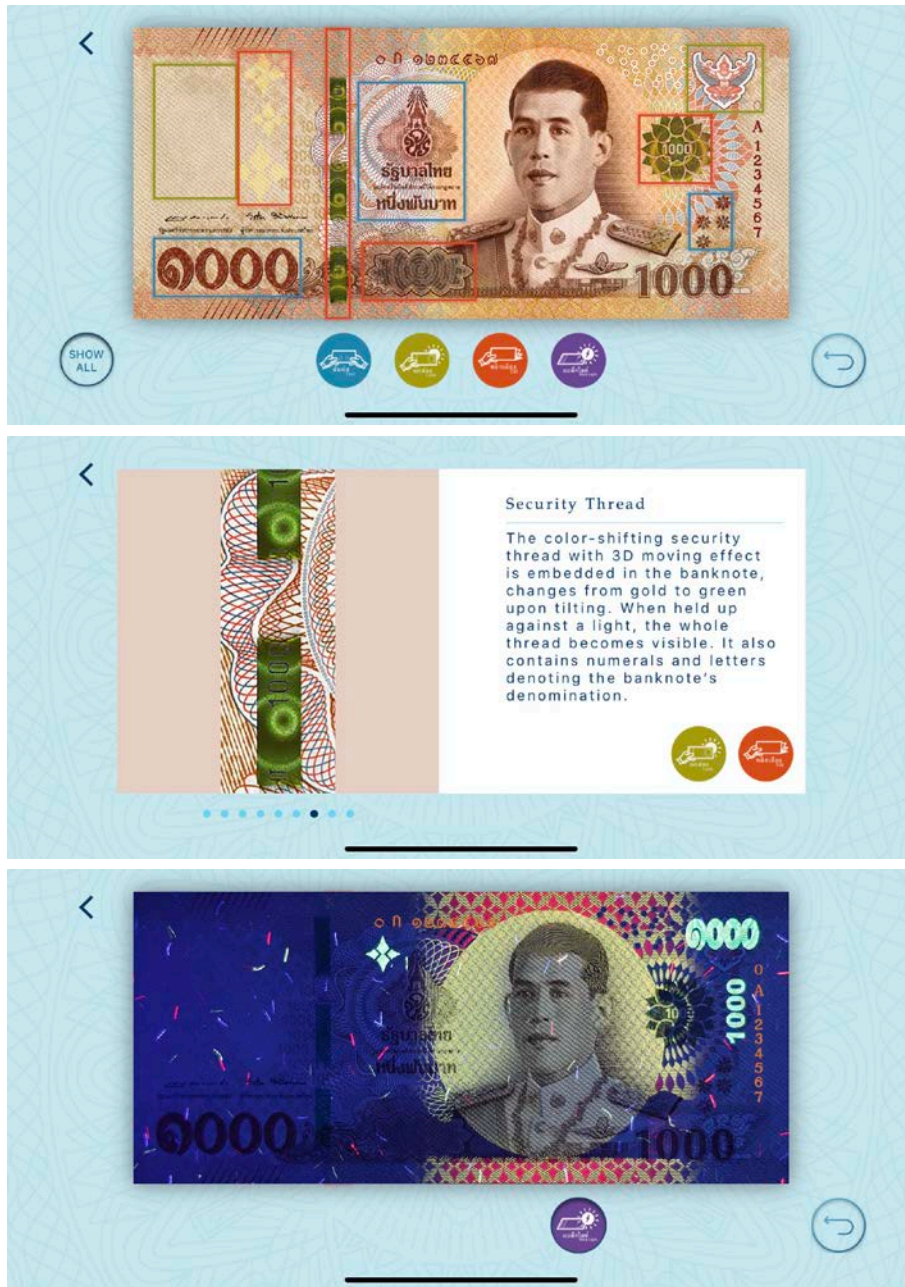


圖 4-4-2 泰國鈔券宣傳 app 畫面擷取
(圖片來源： Thai Banknotes App)

另外瑞典的 app 提供了辨識的功能，但是經過使用實測的結果，必須有高分像度的手機相機功能、良好的光源、另外鈔券不能有折損或是污漬，此外還必須花時間調整等待，不然都絕大多數的辨識結果都會切換至無法辨識的畫面，故其實用性並不高。

此外，由於擴增實境(Augmented reality, AR)可以在真實的畫面中加入 3D 電腦動畫的效果，其具有高度的互動性，故非常容易引起使用者的興趣，近來有些國家的鈔券宣傳 app 均使用了此功能。在 2019 年初，馬拉威儲備銀行推出的 app，不僅利用手機可以替供互動的功能，利用手機內的陀螺儀偵測傾斜來提供使用者互動，在傾斜手機不同角度時交替顯示/隱藏面額以及光影變化安全線，模擬實際辨識的方式。其尚運用最新的 2000 面額鈔票展示擴增實境動畫，其不僅可以引起話題，也可使民眾更有意願去取得該面額鈔票。為了提高下載率，該 app 亦利用社交媒體，在臉書成立官網宣傳，提供 App 教學影片，提供下載連結，另也配合臉書使用者置入業配。

使用此一技術的尚有俄羅斯，在其舉辦的 2018 年 FIFA 世界杯前夕，俄羅斯銀行推出了其首個官方 app，旨在向大眾以及外國遊客介紹目前流通的俄羅斯紙幣。該 app 包含有關目前流通的每張俄羅斯銀行紙幣的資訊，也包括最新發行的世界盃紀念紙幣，其雖然較少被使用於流通，但仍為法定貨幣。

另外使用 app 來宣傳新發行鈔券的例子尚有亞美尼亞。該國在 2018 年 11 月發行第三系列亞美尼亞紙幣，為了跟上防偽印刷的最新發展並促進識別，新的亞美尼亞鈔票配備了現代化且易於識別的新防偽特徵。故為了向民眾宣達，亞美尼亞中央銀行(CBA)與 G + D Currency Technology GmbH 合作，為 Android 和 iOS 智慧型手機開發了教育用 app。該 app 有助於識別鈔票並檢查安全功能。並運用互動的方式說明了如何透過鈔票傾斜、摩擦或通過放大鏡等方式來觀察辨別真偽。它還可以將用戶連接到 CBA 網站，新聞頻道或 YouTube 和 Facebook 頁面，或透過電話或電子郵件聯繫 CBA，並且以亞美尼亞語、俄語和英語提供。

另外 G + D Currency Technology GmbH 尚有開發一個教育 app，但其較少見的將其目標對象設定為兒童，幫助兒童學習鈔票安全功能和設計功能。透過主角—鸚鵡 Penny 以幼兒友善的方式解釋了安全功能；另一個是測試部分，透過測試可和使用兒童有互動，並確認兒童已學得如何識別鈔券的安全特徵。

五、愛沙尼亞晶片身分證 ROCA 安全漏洞之經驗與教訓

愛沙尼亞共和國 (Republic of Estonia) 位於歐洲東北部，是波羅的海三國之一，人口約 130 萬人，1991 年從脫離蘇聯獨立，原本只是個落後的農業國家，地廣人稀，為更有效率地服務全國民眾，所以政府決定將行政作業高度數位化。經過近 20 年來的運作，現在的愛沙尼亞被《Wired》雜誌稱為「世界上最先進的數位社會」，其所建立的電子生態系統有 5,000 多項由政府及私人企業提供之數位服務，包括網路報稅、銀行轉帳、電子投票、申辦電信服務及電子處方簽等，不僅高效、安全且透明。

然而，2017 年 8 月 30 日，愛沙尼亞晶片身份證(以下稱 eID card)發生 ROCA 安全漏洞 (The Return of Coppersmith's Attack, ROCA)，影響約 80 萬名持卡者，若要更換所有實體 eID card 是以往未有的經驗。但是愛沙尼亞卻在隔年 3 月 31 日前完成 94% 的更新，愛沙尼亞政府認為其成功的關鍵是遠端更新、開放式風險管理，以及政府機構與電子服務提供商間緊密的合作，其危機處理過程值得將導入數位身分證之世界各國借鏡。

(一) 愛沙尼亞之數位應用

愛沙尼亞政府自 1997 年開始推動 E 化政府 (e-Government)，希望運用數位科技提升行政效率，先是於 2000 年推出的個人資料交換系統 X-Road 資料庫作為骨幹，又於 2002 年發行 eID card 作為數位化之基礎。此外，領先其他國家的數位概念還包括：電子內閣會議 (E-Cabinet)、數位公民 (e-Residency)、數據大使館 (Data Embassy)，甚至計畫推出由國家發行之虛擬貨幣 (Estcoin) 等。自從積極展開數位改革後，愛沙尼亞近年來已成為歐洲數位化程度最高的國家，更是各國發展晶片身份證的典範。

1. X-Road 資料庫

愛沙尼亞的國家資訊基礎架構是以 X-Road 做為骨幹，起因是政府沒有

一個大型的中央資料庫，但各政府機關及私人企業都有獨自的資料庫，所以藉由區塊鏈技術的概念，各個政府與私人企業的資料庫可以連結、貫穿，藉由強健的資訊系統與通訊協定，彼此資料可以互相分享。民眾的個人資料匯流到 X-Road 資料庫中，只要民眾授權，不必反覆填寫相同的資料，政府機關或私人企業就能從 X-Road 存取，例如從健康保險資料庫調出個人醫療紀錄，實行遠端開藥；或是申辦貸款時可直接授權銀行調出個人基本資料與信用紀錄，不僅節省時間，更降低了紙本作業時所消耗的大量紙張資源。

目前愛沙尼亞國民可透過 X-Road 存取 2,700 多項由政府提供之數位服務，除結婚、離婚及土地買賣須本人至政府機關親自辦理外，99%的公共服務皆已數位化，24 小時皆可在網路上辦理，包括出生登記、電子病歷、稅務申報、創業登記、申請社會福利、查看學業成績、換發駕照、停車位協尋及電子投票等，另包括私人企業的銀行開戶、申請貸款及申請電信服務等，這些數位服務後來被稱為「e-Estonia」，影響公民日常生活，也對其極為信賴。

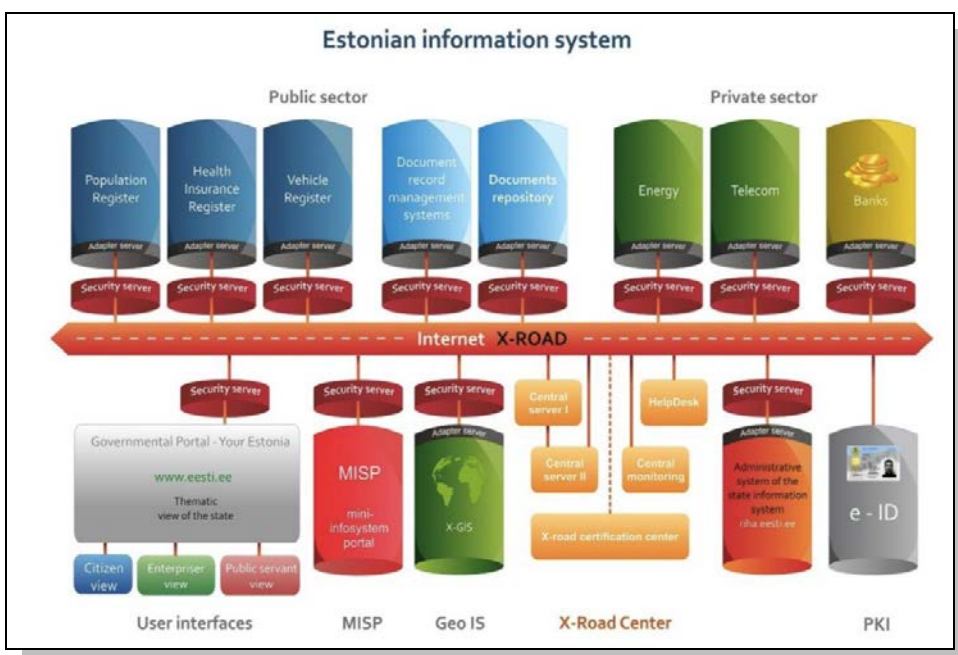


圖 4-5-1 愛沙尼亞 X-Road 架構圖
 (資料來源：愛沙尼亞資訊系統管理局 (RIA) 網站)

2. 晶片身分證 (eID card)

完整的 e-Estonia 數位服務除以 X-Raad 做為數位基礎骨幹，還須加上晶片身分證及數位簽章，才能確保資訊真正的安全。為取信於民，愛沙尼亞政府在 2002 年發行 eID card 前，先於 2000 年制定專法，作為 eID card 發行的法源依據，並在 2002 年通過《數位簽章法》，規定數位簽名與手寫簽名具有相同的法律效力，以加速各類文件簽署完成的速度；而 2017 年通過的《緊急狀態法》，則是規定身份證和數位簽章之認證至關重要。

愛沙尼亞資訊系統管理局 (The Information System Authority, RIA) 隸屬於經濟與通訊部，主要工作是建置愛沙尼亞國家資訊系統的基礎架構，自 2016 年起負責 eID card 上的數位元素，同時也管理 eID card 存取數位服務的政府入口網站 (www.id.ee)，eID card 由警察及邊境保衛署 (Police and Border Guard Board, PPA) 管轄，而數位憑證則是由愛沙尼亞憑證管理中心 (SK ID Solutions) 發行，也負責憑證掛失及查詢憑證是否有效。

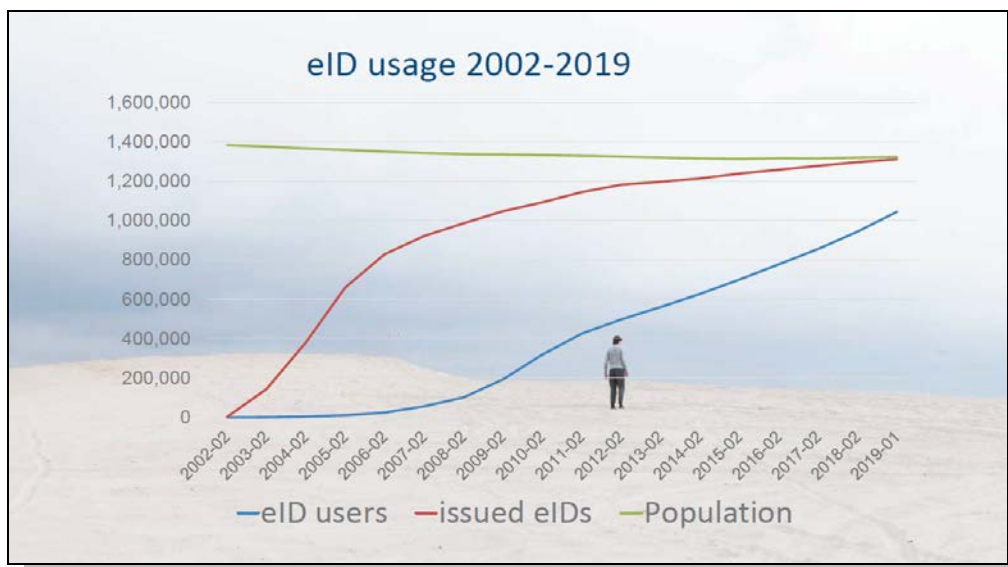


圖 4-5-2 2002 年至 2019 年愛沙尼亞 eID card 發行量
(資料來源：2019 INTERGRAF Copenhagen proceedings)

愛沙尼亞政府於 2002 年首次發行 eID card，但當時的持有率並不高，第一年僅有 10 萬人持有，但發行 17 年來，在政府機關積極推動下，目前

卡片持有率已高達 99%，原因如下：

(1)以強制法規為後盾

愛沙尼亞政府為大力推廣 eID card 政策，一開始便決定採取強制規定的策略，藉由專法規定，除 15 歲以下公民外，其餘每位公民皆須依法強制持有 eID card。

(2)備齊大量便民的數位服務

為擴大 eID card 之運用，愛沙尼亞政府積極強化政府機關及私人企業各項功能之應用，增加民眾使用 eID card 之動機，以 X-Road 串聯所有公、私部門之資料庫，提供 5,000 多項數位服務。正因提供足夠誘因，讓所有民眾看見晶片身分證的便利，致晶片身分證持有普及率逐年增加，例如：

- 愛沙尼亞政府免費釋出 eID card 相關軟體，民眾可自行下載用來簽署或加密數位文件。
- 若愛沙尼亞公民想在海外簽署文件，政府提供相關免費軟體，完成簽署後透過電子郵件傳送，3 分鐘內即可完成整個程序。
- 以往用傳統報稅方式需等待數個月才能退稅，但透過網路報稅，5 天內即可獲得退稅。2015 年，愛沙尼亞政府更進一步推出一鍵報稅機制，個人稅務資料已預先載入報稅系統中，民眾只需要檢查資料正確與否，確定無誤後，按下確認鍵，即可完成報稅作業。
- 愛沙尼亞自 2005 年起開始使用電子投票 (i-Voting)，民眾只需使用 eID card 登入投票系統點選候選人，即可完成投票作業。投票完成後，民眾也可以使用手機查詢，確認是否自己投給心目中的候選人。開票前，系統會自動移除投票者的個人資料，以保障投票的匿名性，即使愛沙尼亞公民散落在全球超過 100 個國家，皆可在遠端透過網路完成投票作業。

(3)政府積極推動與私人企業結合

愛沙尼亞政府將 eID card 相關的程式碼 (Source Code) 公開至開源軟體程式碼平臺 GitHub，降低私人企業將自家系統或產品整合至 eID card 系統之門檻。

私人企業建立自己的數位服務，並且透過 eID card 進行認證，例如，銀行以 eID card 作為服務憑證，也投資金錢協助愛沙尼亞政府建立數位憑證機制，私人企業直接利用國家發行的晶片身分證作為服務憑證，不必開發自己的憑證工具，可降低成本，創造雙贏的局面。

(4)持續增進資安防護

愛沙尼亞的 eID card 上只登載持卡人姓名、性別、出生日期及紙本簽名，數位簽章則儲存在晶片中，即使持有卡片，仍得搭配 PIN 碼才能使用。

而且為預防晶片身分證遭非法冒用，愛沙尼亞 eID card 使用「公開金鑰基礎建設 (PKI)」加密，原 2002 年發行的晶片身分證金鑰長度採 1024 位元，但目前發行版本的 PKI 金鑰長度已有 2048 位元，按現在的需求標準，不僅安全度足夠，破解困難，更能確保國民的隱私安全。愛沙尼亞的 eID card 由警察及邊境保衛署 (PPA) 核發，無論是身分證、居留證皆採取相同的資安技術，即 PKI X.509 安全憑證之兩組金鑰。X.509 憑證是由國際電信聯盟 (ITU-T) 制定之認證標準，以公開金鑰基礎架構 (PKI) 與數位簽章為基礎。

另外，愛沙尼亞原採 RSA 加密演算法，在經歷 2017 年安全漏洞 (ROCA) 事件後，現在採用更加安全的橢圓曲線加密演算法 (Elliptic curve cryptography, ECC)，持續增進 eID card 的資安強度。

(5)資訊系統及政策公開透明

愛沙尼亞政府為取得人民信任，將 eID card 相關系統的程式碼 (source code) 公布於開源軟體程式碼平臺 GitHub 上，任何人皆可檢視這些程式碼，一旦開發者發現系統程式碼存在漏洞或破綻，皆可向上通報相

關機構要求修復。

此外，愛沙尼亞政府亦建立透明的查核機制，政府存取個資都會留下相關的 Log 紀錄，若民眾不清楚政府存取私人資料的理由，可透過自動化系統馬上提出申訴，減少人為介入。而 eID card 專法中，亦針對不同隱私程度的個人資料，規範可公開或不公開的原則。

(6)全球首座數據大使館（Data Embassy）

愛沙尼亞曾在 2007 年遭受俄羅斯大規模的駭客攻擊，導致當時政府、銀行以及許多網站停擺。為確保公共服務功能及安全性，愛沙尼亞於 2015 年啟動「數位大使館」的概念，並在 2017 年與盧森堡簽署最終協議，於 2018 年在盧森堡設立全球首座 4 級安全級別（數據設施的最高級別）的「數據大使館」，是用來備份國民身分證、稅金、年金、不動產、企業登記及法規等國家級數位資料之海外數據中心，未來即使政府受到網路攻擊，也能隨時存取所需的資料。



圖 4-5-3 愛沙尼亞晶片身分證（eID card）

晶片身分證不會儲存隱私資料，亦無法作為付款工具，它主要是用來辨認用戶的身分，作為存取數位服務的鑰匙，而且必須配合數位簽章及密碼才能使用。

當持卡人遺失 eID card 的兩組 PIN 碼時，只需至政府服務據點或銀行等機構申請新密碼；若持卡人密碼遭竊，民眾也可透過政府提供之免費軟

體修改密碼。實體 eID card 一旦遭竊、遺失，民眾可在任何時間撥打政府服務電話，要求註銷卡片憑證，中止該 eID card 之存取權限，避免被不法人士盜用。當市民完成卡片註銷程序後，系統後端資料庫除移除該卡憑證之效力，也會註記這張卡已遭竊，若有人試圖使用它非法跨越國界，立即會被發現。

現在的愛沙尼亞 eID card 是各項數位服務之關鍵基礎建設，它是身份證明文件和國民健康保險卡、亦可用於電子投票 (i-Voting)、醫療電子處方、檢查病歷及稅務申請等，同時也是歐盟各國間的合法旅行證件。截至 2019 年底，有關愛沙尼亞數位化的數據如下（資料來源：e-estonia.com）：

- 99%愛沙尼亞居民領有 eID card
- 愛沙尼亞居民使用 Mobile ID 224,570 人（約占 17%）
- 愛沙尼亞居民使用 Smart ID 463,559 人（約占 35%）
- 67% 愛沙尼亞居民定期使用身份證
- 2002 年 10 月 7 日用身份證簽署的第一份檔案
- 2002 年起，數位簽章發放次數 700,000,000 以上
- 2,773 項服務可通過 X-road 使用
- 1 個月內通過 x-Road 進行的查詢數量 180,855,017 次（2019 年）
- 2019 年使用網路投票參與人數百分比 43.8%
- 62,000 人申請電子居住 (e-Residency)，來自 165 個國家/地區
- 從 2005 年開始使用電子投票 i-Voting
- 愛沙尼亞居民使用 i-Voting 比例 44%；投票來自 110 多個國家
- 99%的患者擁有電子健康記錄
- 99%的藥物都是電子處方
- 100%電子醫療賬單
- 98%線上稅務申報
- 3 分鐘完成線上繳稅
- 99%網路銀行交易
- 98%在線上申請設立公司

(二) 愛沙尼亞 eID card ROCA 安全漏洞

1. 原由

2017 年 8 月 30 日，愛沙尼亞政府接獲一名來自捷克馬薩里克大學（Masaryk University）密碼學暨安全研究中心（Centre for Research on Cryptography and Security, CRoCS）研究員的通知，告知愛沙尼亞 eID card 所使用的晶片存在安全性漏洞。根據該研究小組的分析，這一國際上稱為 ROCA（Return of the Coppersmith Attack）的漏洞來自於德國半導體製造商英飛凌科技公司（Infineon Technologies AG）所生產的晶片，該晶片使用的加密庫，會產生脆弱的 RSA 金鑰對。而英飛凌正是愛沙尼亞 eID card 供應商金雅拓公司（Gemalto）的供應商，影響愛沙尼亞自 2014 年 10 月起發行約 80 萬張的身份證，約佔整體發行量的三分之二。

2. ROCA 安全漏洞之影響

此 ROCA 漏洞發生於英飛凌自 2012 年以來推出的 SLE 78 系列晶片，其信賴平台模組（TPM）的加密庫含有安全漏洞。可信賴平台模組是一種安全加密處理器的標準，也是電腦安全體系結構的基礎，主要用來儲存諸如密碼、憑證與加密金鑰等重要資料，以專用微控制器的形式於裝置上嵌入加密金鑰，以保障硬體的安全，它通常被安裝在筆電、路由器或物聯網（Internet of Things, IoT）裝置的主機板上。

據估計，全球至少有 10 個國家採用此款晶片，包括斯洛伐克、奧地利、波蘭、保加利亞、科索沃、意大利、台灣、西班牙、巴西及馬來西亞等，共有超過 10 億個晶片受到影響，它們被用於身份證件、護照、駕駛執照及門禁卡等各式身分證明文件。該漏洞可能波及的對象還包括：

(1) 硬體裝置

受到影響的廠商包括 Google 的 Chrome、微軟（Microsoft）、聯想（Lenovo）、惠普（HP）、東芝（Toshiba）和富士通（Fujitsu）等，皆盡

速展開漏洞修補措施，包括發布軟體更新或漏洞解除指引等，例如 Microsoft Windows 中，TPMs 用來保護 BitLocker 磁片加密和作業系統中的其他安全機制，Microsoft 通過 Windows 例行性更新發佈一個臨時修補程式（patch），以軟體解決方案取代 TPM，而其他製造商也發佈類似的修補程式。

(2) 身分驗證設備

用於身份驗證或安全權杖（Security token）之設備廠商也受到牽連，其中包括 Yubico 和 Gemalto。身分驗證設備主要用於虛擬私人網路（Virtual Private Network，VPN）訪問、電子郵件安全及其他關鍵安全操作等。而 Yubico 的做法則是發佈一個檢查工具，只要是韌體版本為 4.2.6 至 4.3.4 間的 YubiKey 4、YubiKey 4C 及 YubiKey 4 nano 的產品，若經民眾確認，皆可免費更換。

(3) 支付卡

一些帶有晶片的支付卡也有可能受到攻擊。

雖然愛沙尼亞只有約 80 萬張的身份證受到影響，在全世界 ROCA 漏洞影響的占比微乎其微，然而，其他國家對電子服務系統的依賴程度遠低於愛沙尼亞，因此愛沙尼亞政府對於此次 ROCA 安全漏洞的危機處理方式至關重要。

3. ROCA 安全漏洞之技術細節

此 ROCA 漏洞發生於英飛凌自 2012 年以來推出的 SLE 78 系列晶片，而愛沙尼亞所使用的晶片正是該系列的 1.2.13 版本，其可信賴平台模組（TPM）的加密庫含有安全漏洞，再加上採用 RSA 演算法，會產製出易被破解的金鑰，以致駭客可能使用公鑰進行因數分解重建私鑰。而私鑰主要用於身份驗證和數位簽章，一旦被破解，無需實體卡片即可竊取數位身份，偽裝成合法用戶對文件進行數位簽章、進入電子服務系統，以及解密已加

密的檔案等風險。

RSA 是一種最常被使用的非對稱加密演算法，主要用於加密、身份驗證與數位簽章，在公鑰加密標準和電子商業中被廣泛使用。發生此 ROCA 漏洞的晶片運算採用常數（constant），而非隨機數（random），以致產製出脆弱的金鑰。RSA 常用的金鑰長度有 1024 位元及 2048 位元兩種，而愛沙尼亞所使用的是 2048 bits。

但實際上，要利用該漏洞犯罪並不容易，必須擁有密碼學、軟體設計及卓越的計算能力等大量專業知識。由於運算需要資源，因此要破解私鑰也不便宜。據 CRoCS 估計，若要破解 512 位元的 RSA 金鑰只需花費 CPU 兩小時，成本只要 0.6 美元；破解 1024 位元的 RSA 金鑰則需要 97 天，成本介於 40 至 80 美元間；而破解 2048 位元的 RSA 金鑰則需 140 CPU 年，成本最高，需要花費 2 萬至 4 萬美元。以此次愛沙尼亞使用的英飛凌晶片為例，其由常數產生的 2048 位元 RSA 金鑰，破解時間需要 140vCPU 年，耗電成本約需 2,500 歐元；若是由隨機數產生的 2048 位元 RSA 金鑰，破解時間則須 6442450944000000 vCPU 年，難度及成本皆極高。

表 4-5-1 破解不同複雜性 RSA 金鑰所需時間與成本

金鑰運算方式	破解時間及成本
由隨機數產生的 2048 位元 RSA 金鑰	6442450944000000 vCPU 年
由常數產生的 2048 位元 RSA 金鑰 (即愛沙尼亞使用的英飛凌晶片)	140 vCPU 年
耗電量成本	約 2,500 歐元

(資料來源：2019 INTERGRAF Copenhagen proceedings)

4. 解決方案

ROCA 漏洞發生後，受影響的憑證眾多，且被廣泛使用在政府及私人企業的電子服務中，一旦撤銷這些憑證，將對電子醫療系統、稅務海關局、

政府檔案交換平臺及金融交易等數位服務造成極大的影響，政府機關間的工作也會中斷，因此必須在不影響電子服務提供的情況下，盡快恢復 eID card 的安全性。

愛沙尼亞資訊系統管理局（RIA）自 2017 年 9 月初開始與警察及邊境保衛署（PPA）及其他單位夥伴組成危機處理團隊，在清楚釐清事件根本原因後，決定在不更換實體卡片之情況下，暫停受影響之憑證，且提出以下解決方案：

(1)公眾溝通保持透明

愛沙尼亞政府一開始便決定於第一時間對外說明實情，以取得民眾信任，降低潛在的疑慮。

(2)關閉公鑰資料庫（LDAP）

為確保民眾身分隱私，愛沙尼亞政府嚴加管控 eID card 公鑰資料庫之存取權限，使潛在的攻擊更加困難。

(3)以 ECC 演算法取代 RSA 演算法

橢圓曲線加密演算法（Elliptic Curve Cryptography，ECC）是基於以橢圓曲線理論為基礎的一種非對稱加密演算法，將橢圓曲線中的加法運算與離散對數中的模乘運算相對應，即可建立基於橢圓曲線的對應密碼體制。ECC 的基本運算比 RSA 複雜很多，破解難度更大，所以更為安全。ECC 可使用更短的金鑰長度，來實現與 RSA 相當或更高等級的安全，據研究，160 位元的 ECC 加密安全性相當於 1024 位元的 RSA，210 位元的 ECC 加密安全性相當於 2048 位元的 RSA，所以 ECC 相較於 RSA 有以下優勢：

- 相同密鑰長度下，安全性能更高
- CPU 需求少，運算量小，處理速度快
- 記憶體需求較低，存儲空間佔用小
- 頻寬要求低

(4)啟用遠端更新

自 2017 年 10 月 25 日起，愛沙尼亞的民眾可以從任何配備 eID card 讀卡機的電腦連接到網路，遠端更新其 eID card 軟體，以及暫停可能受影響的憑證。

(5)推廣 Mobile-ID 作為替代方案

Mobile-ID 是允許民眾使用手機作為 eID card，無需使用讀卡機，即可用於電子服務或對文件進行數位簽章。Mobile-ID 的系統是基於特殊的移動 SIM 卡，私鑰與提供身份驗證和簽名功能之應用程式一起存儲在移動 SIM 卡上（憑證格式為 ITU-T X.509；金鑰格式為 RSA2048 和 ECC384）。客戶須自行向電信業者申請移動 SIM 卡，前提是已領有 eID card 的民眾，才可以申請 Mobile-ID。

(6)暫停發放憑證

2017 年 11 月 3 日，愛沙尼亞警察及邊境保衛署（PPA）宣布暫停發放自 2014 年 10 月 16 日至 2017 年 10 月 25 日間發行受 ROCA 漏洞影響約 80 萬張 eID card 之憑證，並要求持卡人在 2018 年 3 月底前須對其 eID card 進行更新升級。

(7)撤銷憑證

2018 年 4 月 1 日，撤銷受 ROCA 漏洞影響，但尚未更新之憑證。

(8)公共風險管理

愛沙尼亞政府對於透過對公共風險的識別、衡量和控制，而以最小的成本使風險所致損失達到最低程度，提高對突發事件風險的預見能力和突發事件發生後的救治能力，保護公民的生命和財產安全維護社會穩定，及時有效地防控公共風險，同時在風險控制中把握機會，化風險為機遇，此次 ROCA 漏洞危機為公共風險管理做了最好的示範。

(9)公、私部門密切合作

政府機構與電子服務提供商間緊密的合作，迅速開發更新軟體。

5. 結果

所幸，在撤銷受影響憑證的過程中，並無攻擊事件發生，憑證撤銷後，愛沙尼亞政府將私鑰重構為概念驗證樣本（Proof of Concept；PoC）。在完善的危機處理下得到以下結果：

(1) 5 個月內更新 500,000 張卡

更新軟體上線不到一個月，已有將近一半的 eID card 得到更新，在更新的 494,000 張 eID card 中，有 354,000 張（約 72%）採遠端更新。

(2) 2018 年 3 月 31 日前撤銷 26 萬張卡片之憑證。

(3) 經過更新的卡片目前仍在使用中，將可繼續使用至 2023 年 11 月。

(4) 所有的電子服務都支援更新後（改採 ECC 加密演算法）之卡片。

(5) 替代方案——Mobile ID 使用率提高

ROCA 漏洞的發生並沒有影響到 mobile ID，但事件發生前只有約 10 萬人使用它，許多電子服務不支援它。但事件發生後，mobile ID 使用量增加，支援的電子服務也更多。

(6) 2018 年 12 月底前仍發行相同晶片的卡片

值得一提的是，2017 年 10 月的地方選舉中，有 31.7% 選民使用電子投票，人數創下以往的紀錄。在接下來的幾週內，使用 eID card 進行交易的次數一樣保持在正常水準，而且 2018 年 2 月提供 1,000 萬個數位簽章，相較於 2017 年同月份的 600 萬個數位簽章，不減反增，表示在 ROCA 漏洞發生的過程中，民眾對 eID 的信任並未受損。

6. 經驗與教訓

eID card 的資安漏洞危機說明愛沙尼亞社會對數位基礎設施的依賴，愛沙尼亞危機管理工作中必須特別審核的流程，包括身份證管理、風險評估和緩解，以及機構間合作，而且考慮到該漏洞對全球之影響，愛沙尼亞需要對跨公私部門得出國際性的結論。

(1)資訊共享和漏洞披露

正常的預期危機訊息來源應該是來自國際通知機制或供應商的通知，但此次愛沙尼亞 ROCA 的資安危機卻是從一個國際研究小組成員所提供的資訊而得知。有人認為，通知機制是為具有明顯影響事件而設計，因此不適合處理危機早期階段之攻擊，因此該案例讓愛沙尼亞政府重新審視供應鏈管理和通知機制。

特別的是，歐盟成員國可能比較希望《電子身分認證與信賴服務規章》（eIDAS）第 19 條的解釋和出現新的做法。總體而言，必須評估通報機制中可能存在的差距，並且共同解決國際風險和漏洞共享的國際慣例。

(2)風險管理和持續性計劃

愛沙尼亞 eID card 為 5,000 多項政府及私人企業提供之電子服務提供身分認證和數位簽章。在大多數情況下，面對面身分驗證和手寫簽名不再是可接受的選擇，因此，規劃 eID card 替代方案，必須考慮支援各項電子服務，對政府及私人企業而言，這是對風險管理和持續性規劃有用的案例。

即使可以遠程更新和暫停認證，但如果身份證韌體中沒有嵌入多個加密庫，愛沙尼亞也會受到更嚴重的影響。

(3)政府引入創新的任務

政府機構始終面臨著內部開發技術或從市場採購新技術的兩難困境，很少有政府具備全部必要的技能，大多數能力都在於私人企業，政府只是客戶，無法完全解決技術上原本就有的問題。因此，除供應鏈管理和業務連續性規劃外，政府還可以在開發、採購和認證技術方面發揮其影響力。

(4)開放性

如果沒有公眾和媒體等利益相關者的參與，便無法管理數位基礎設施的資安漏洞所產生的風險。國家、國際和企業利益相關者間具有不同

的期望、角色和準備程度，需要廣泛合作，才能為長期解決辦法奠定基礎，使之能夠克服尚未出現的問題。

表 4-5-2 愛沙尼亞數位身份證 ROCA 危機處理時間軸

時 間	危機處理進度
2017 年 8 月 30 日 晚上 7 點 35 分	<ul style="list-style-type: none"> • 國際密碼學研究小組的一名成員向愛沙尼亞資訊中心（CERT-EE）發送一份正式通知，內容涉及與愛沙尼亞 eID card 相關的英飛凌晶片之安全性漏洞。 • 風險來自 RSA 金鑰對生成中使用的加密庫漏洞。 • 該漏洞可能影響自 2014 年 10 月起愛沙尼亞簽發約 80 萬張的 eID card。
8 月 31 日	愛沙尼亞資訊系統管理局（RIA）初步評估後確認該漏洞的可能性，並向員警和邊防警衛局（PPA）以及經濟事務和通信部通報情況。
9 月 1 日	<ul style="list-style-type: none"> • 經濟事務和通訊部長聽取關於此事件之簡報。 • 由 RIA 負責人召集政府、外部技術專家及私營部門（Cybernetica、Nortal），組成戰略危機管理團隊。
9 月 3 日	<ul style="list-style-type: none"> • 總理和其他有關部長會面。 • RIA 和 PPA 工作組評估情況和影響，並提出建議。
9 月 4 日	<ul style="list-style-type: none"> • 政府舉行特別會議。PPA、RIA 和其他機構組成媒體和戰略溝通人員。銀行和電信等公、私營部門之利益相關者皆收到通知。 • 關閉憑證公共資料庫（LDAP）。
9 月 5 日	<ul style="list-style-type: none"> • 通知國際合作夥伴此漏洞之存在。 • 總理、企業家和資訊技術部長，以及 RIA 和 PPA 的負責人舉行聯合新聞發佈會，向民眾彙報情況。 • RIA、PPA 和 SK ID 通力合作，不斷更新 www.id.ee 網站資訊。
9 月	各工作小組集中於技術解決辦法、危機管理、法律和溝通，並定期舉行會議。根據需要，另外邀請其他機構和其他外部專家參與。
10 月 5-11 日	舉行市政選舉。使用網路選舉選民的參與率創下了歷史新高。透過網路投票人數占所有參與者的 31.7%，略高於以往的選舉。
10 月 16 日	該漏洞影響 Microsoft、Google（Chrome OS）、Yubico、Gemalto 和一些大型電腦製造商（如聯想和富士通），皆發佈安全報告。

10月25日	<ul style="list-style-type: none"> • 開始發行採 ECC 加密演算法的新 eID card。 • 愛沙尼亞 eID card 線上更新的測試期開始。 • 在六天的測試中，有近 20,000 個受此漏洞影響的身份證被更新。
10月31日	<ul style="list-style-type: none"> • eID card 更新服務所需的流量很大，導致遠程更新方案當機。 • 系統在 11 月 2 日前穩定下來。 • 斯洛伐克撤銷 6 萬張帶有 ROCA 漏洞的證書，持卡人必須申請新卡。
11月1日	西班牙共撤銷 1,700 萬張受影響的卡片。
11月3日	<ul style="list-style-type: none"> • 暫停發放受影響之 eID card 憑證，約有 74 萬，但可上網更新，使其可再次以電子管道使用。 • 此外，PPA 另開設額外的服務辦公室來更新證書。
11月5日	<ul style="list-style-type: none"> • 使用電子服務統計資料顯示，受影響憑證的暫停並未導致 eID card 使用量下降。 • 電子居民的數位交易反而增加。
2017 年終	共更新 40 萬張身份證。mobile ID 和 Smart ID 使用者的數量及使用電子服務的項目皆有所增加。
4月1日	<ul style="list-style-type: none"> • 尚未更新的證書將被註銷，且不能再以電子方式使用。 • 94%的電子身份證已經更新。

(資料來源：2019 INTERGRAF Copenhagen proceedings)

六、區塊鏈對安全識別的潛在影響－於電子投票之應用

區塊鏈技術 (Blockchain) 因加密貨幣而受到矚目，自出現以來便受到好壞參半的評價，支持者將其視為革命性的、不具權威性、是真正獨立的；而批評者在意的包括洗錢和盜竊等潛在風險，以及另一個泡沫化。因此，要達成數位政府 (e-Government) 的目標，必須了解區塊鏈技術之真正核心，研究具代表性之案例，才能為未來發展做出正確的規劃。

(一) 什麼是區塊鏈系統？

區塊鏈不僅是一種技術，更是觀念上的改變，例如傳統上兩個陌生人的

交易，需要有第三方作為仲介或擔保才能完成，而套入區塊鏈技術後，可以直接交易而無需中間機構的存在。區塊鏈存在許多有別於傳統思維與中心運作的特性，包括：去中心化、匿名性、不可篡改、講求共識、加密安全性等 5 大優勢。

1. 區塊鏈是一個去中心化的系統

區塊鏈優勢最重要的核心概念是「去中心化（decentralised）」，其運作不需依賴第三方，而是靠一個個節點（nodes），又稱為礦工（miner），只要願意貢獻電腦硬體運算能力，鏈上的所有人皆可成為可以驗證的節點。節點對區塊進行運算加密後，經所有區塊鏈上的人確認後上鏈，產生的新區塊會再公開到所有人的區塊鏈上，這種驗證機制稱為工作量證明（Proof-of-Work，PoW）。每個人在區塊鏈中的權限是相等的，任何人都可以公開查詢，以獲得區塊鏈中的數據，正因為交易公開，一旦被更改資料便會被其他人發現，因此大幅提升惡意竄改之難度。

區塊鏈技術藉由密碼學（Cryptography）及分散式雜湊函數（Hash Function）確保了交易的安全性及不可篡改性。其所採用的公鑰密碼學（Public Key Cryptography），又稱非對稱式密碼學（Asymmetric Cryptography），如 RSA 或 ECC 演算法來加密資料，公、私鑰匙都可以進行加密（encryption）或解密（decryption），但只有成對的公、私鑰可以互相加、解密，用以確認身分。而雜湊函數是以十六進位為基礎，各種檔案經過壓縮後成為一連串大小相同的密碼，具有產出迅速、不易重複及單向（one-way）的特性，所以不可能被竄改。因此，有公、私鑰確認身份，以及雜湊函數迅速產生單向加密數字，便可解決最令人擔憂的網路安全信任問題，即使不依賴第三方，也可讓使用者達成共識，以非常低的成本解決網路上信任與資料價值的難題。如上所述，區塊鏈的特色歸納為以下幾點：

(1) 維護持續成長的資料清單

(2) 記錄經過強化，以防止篡改和修訂

- (3)加密證明，而不是對中心的信任
- (4)通常沒有中央權威
- (5)節點之間互不信任

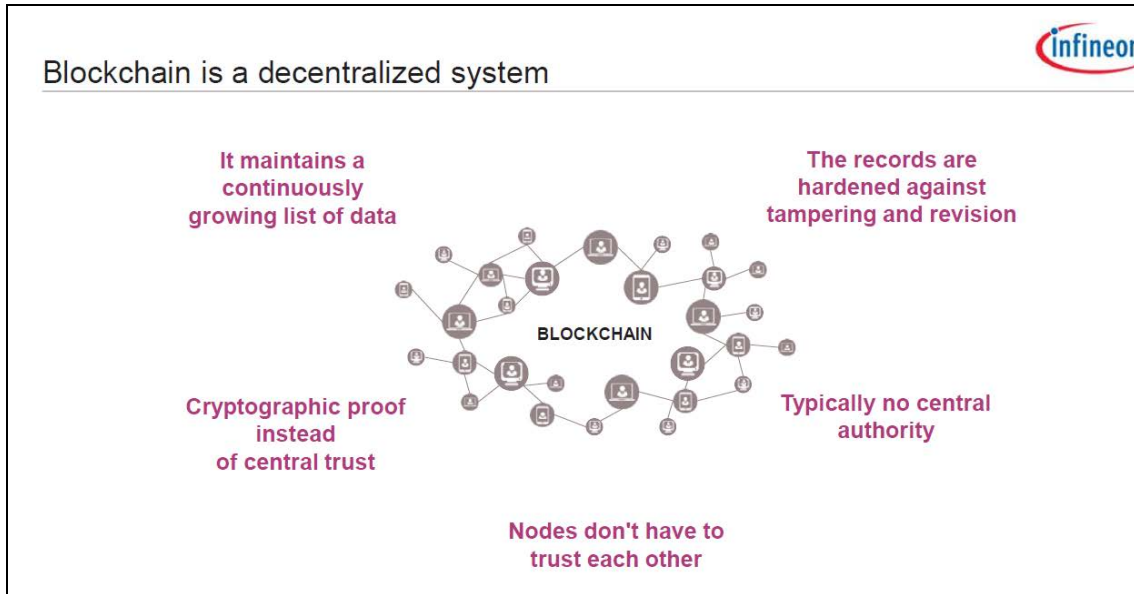


圖 4-6-1 區塊鏈去中心化系統

(資料來源：2019 INTERGRAF Copenhagen proceedings)

2. 區塊鏈之應用領域

採區塊鏈技術可避開「信任」的問題，即使大家在互不認識、互不信任的狀況下，也能透過共識協議一起合作，並保證運作過程公開透明，所有記錄不能造假，而且可隨時驗證，所以區塊鏈適用的範圍很廣，包括物流業、消費者、能源業、汽車業、資產與契約管理及加密貨幣等領域。

區塊鏈就技術面來看，它是一個分散對等的資料庫，資料藉由分散式節點進行數據的儲存、驗證及傳輸，形成一個大型的公共事務筆記本（分類帳）；就商業面來看，它是一個在用戶間交換價值的網絡；就法律面來看，它是一個無第三方交易的驗證機制。

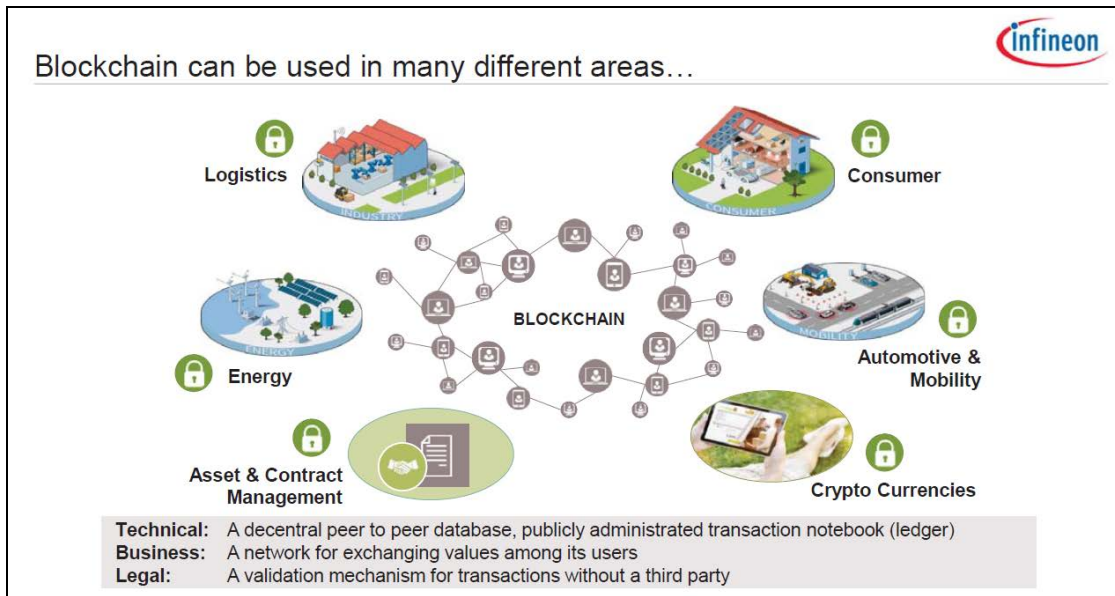


圖 4-6-2 區塊鏈之應用範圍

(資料來源：2019 INTERGRAF Copenhagen proceedings)

(二) 區塊鏈是否適合安全政府應用？

1. 集中和分散系統

民眾從事金融交易時，通常是由政府或金融機構為中介者，確保借貸、匯款或轉帳等交易，其結構像是「B2C (business-to-customer)」，由一個權限比較大的人或機構來管理大多數權限小的人，作為可信任和替他人背書的第三方，例如銀行與客戶，或是臉書與使用者。

而區塊鏈則是一種跳過第三方中介的「P2P (peer-to-peer)」網路關係，支付過程可直接由一方發起，支付給另一方，不需再透過第三方管理機構和硬體設施作為中心機制，因此可避免如銀行破產、社群或網站任意更改使用者功能或販賣用戶資料等問題。

區塊鏈科技在比特幣 (Bitcoin) 和以太坊 (Ethereum) 等領域之應用已廣為人知，其主要思想是分散信任，不將控制權和管理權交給某個單位，而是由整個社區定義關鍵價值，並將其分佈在多個代理或節點中，即所謂的共識，由於缺少中央實體，該機制被認為是區塊鏈系統的民主基礎。由傳統眾人遵守規則到共識規則 (Consensus Rules)，是否為民主的展現？鑑

於此種「民主」性質，區塊鏈技術被視為可運用於電子投票機制中——即實施民主制度最重要的工具之一。

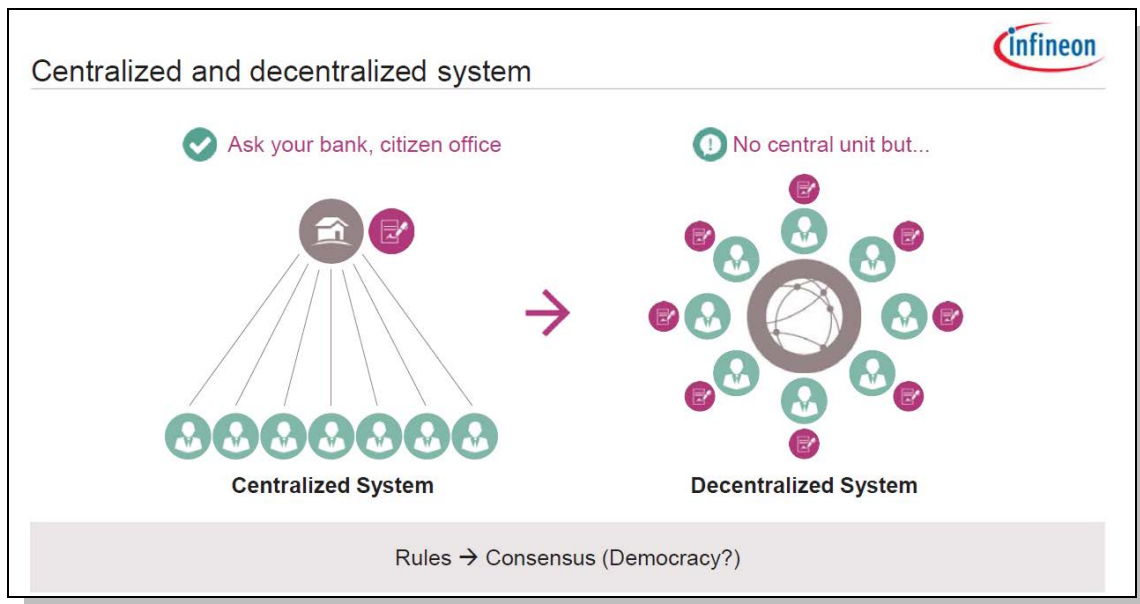


圖 4-6-3 區塊鏈集中和分散系統概念圖
(資料來源：2019 INTERGRAF Copenhagen proceedings)

2. 簡化的區塊鏈交易流程

區塊鏈技術簡言之，是「一個建立在 P2P (Peer-to-Peer) 網路架構的分散式帳本系統」，可將它理解為一個全民皆可參與的電子記帳本，一筆筆的交易資料皆可被記錄，而且透過集體維護，可讓區塊鏈裡的資料更為可靠。由圖 4-6-4 可看到區塊鏈的基本運作：

- (1) A 想把錢匯給 B
- (2) 交易在線上表示為「塊」
- (3) 該塊廣播到網絡中的每一方
- (4) 交易在線上表示為「塊」
- (5) 然後可以將該「塊」加到鏈中，進而提供一個不可磨滅且透明的交易記錄
- (6) 錢從 A 轉(移動)到 B

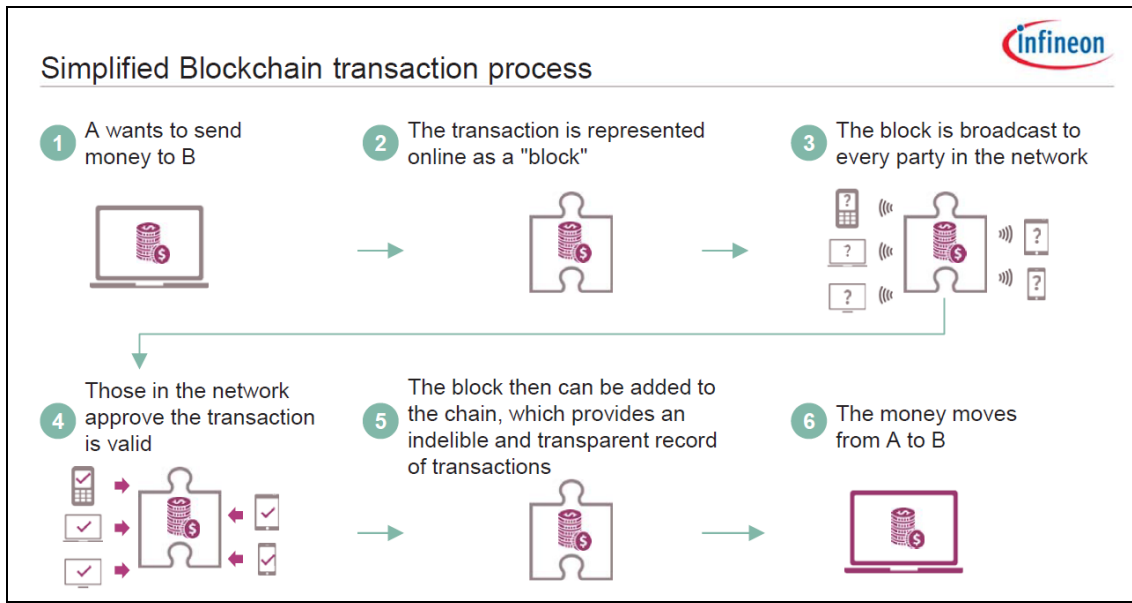


圖 4-6-4 簡單的區塊鏈交易流程

（資料來源：2019 INTERGRAF Copenhagen proceedings）

3. 區塊鏈透過去中心化可為數位應用程序提供信任

(1)傳統的應用程序依靠中央機構，而區塊鏈技術的總體目標是通過分散和冗餘存儲資訊，分別執行事務，為數位應用程序建立信任。

(2)分散式分類帳允許透過共同協商的系統狀態和審查交易。

(3)區塊鏈透過數位簽章、雜湊函數及共識機制等加密方法，為參與者提供數據之完整性和匿名性。

4. 集中投票與分散投票方案

區塊鏈在網路上的數據皆是加密且匿名的，而這些特點能夠降低選票被操縱之可能性，有助於投票機制的改善。傳統的中央投票和數位分散投票方案在投票程序之比較，詳表 4-6-1。

表 4-6-1 集中投票與分散投票比較表

投票程序	集中投票	分散投票
識別/認證	必須在投票過程外單獨執行，確保只有符合條件的人才能投票。	
投票	進行電子投票取決於政府（中央）或區塊鏈實體提供的數位簽章/身份，以確保匿名性並防止私鑰欺詐。	
收集與儲存	由政府機構集中收集和存儲投票結果	在區塊鏈節點上去中心化和冗餘存儲加密選票
清點	單一可信機構統計投票並發佈結果	分散式分類帳允許分散計數和公開審核結果

（資料來源：2019 INTERGRAF Copenhagen proceedings）

5. 選舉中的利益相關者（Stakeholders in election）

選舉中的利益相關者，政府、系統供應商及選民，在主要需求/要求、態度及影響力各有不同，詳表 4-6-2。

表 4-6-2 選舉中的各利益相關者

準則	政府	系統供應商	選民
主要需求/要求	<ul style="list-style-type: none"> 政府決定選舉程序 遵守法律 經濟和生態原因 	<ul style="list-style-type: none"> 商業機會 法規框架和標準（態度） 	<ul style="list-style-type: none"> 方便 隱私/匿名 過程中信任 技術經驗
態度	<ul style="list-style-type: none"> 根據政治動機 立法週期依賴性 	<ul style="list-style-type: none"> 正面-新玩家 負面-取代 	取決於社會人口參數
影響力	高	中	低

（資料來源：2019 INTERGRAF Copenhagen proceedings）

（三）區塊鏈應用中的安全風險

如上所述，區塊鏈應用採非對稱式密碼學，只有成對的公、私鑰可以互相解密，且每個公鑰都由一個私鑰產生，公鑰用於導出地址並驗證簽名，私鑰則是用來生成簽名並簽署交易紀錄。一旦私鑰被盜，駭客將擁有所有資產

的完全訪問權限，用戶會所有資產丟失，難以復原。而區塊鏈交易讓駭客最有利可圖的部分是其不可竄改性，一旦交易被寫入區塊鏈，便不能被撤消、追回，這也是區塊鏈最被詬病和疑慮的部分。

全球前四大會計事務所——英國安永會計師事務所(Ernst&Young)於2018年初發表有關投資虛擬貨幣風險之研究報告，指出2015年至2017年間，有超過372個首次代幣發行(Initial Coin Offering, ICO)計畫，共募得37億美元，但受到駭客攻擊而被盜取或損失之價值逾10%，約4億美元。報告中強調，駭客大部分是透過網路釣魚盜取，即通過點擊惡意連結所致，還有部分駭客直接竊取使用者的私鑰，直接從錢包和交易平台竊取資金。根據該報告資料統計，駭客每月都會從ICO資金中竊取150萬美元。

由此可知，私鑰必須始終保持機密，定期進行備份，私鑰存儲則需要盡可能好的保護，硬體裝置安全性是至關重要的關鍵之一。

(四) 關鍵要點

1. 區塊鏈之保密性和匿名性等特性，可滿足選舉原則之關鍵要求。
2. 區塊鏈技術應用於電子投票，可提高選舉程序中之信任、透明度和效率，同時可降低欺詐之可能性。
3. 區塊鏈熱潮已降低，技術成熟期可能還需要5-10年，但全球對該技術應用於電子投票之效用和可行性仍有高度關注。
4. 區塊鏈技術應用於電子投票，與其說是技術問題，不如說是一個政治和法律問題，因為選舉程序和監管框架取決於政府對公開透明選舉的態度。
5. 投票者之憑證管理是區塊鏈系統中安全身份驗證應用之關鍵。

(五) 結論

電子投票通常採「智慧合約(Smart Contract)」機制，它是以數位形式定義承諾，讓參與雙方可以執行承諾協議，其特色是合約內容透過電腦自動

執行，可避免人為因素造成的糾紛，但智慧合約是由一連串代碼組成，而不是法律條文，因此並沒有法律效用。智慧合約典型的平臺是以太坊 (Ethereum) 和 Corda，使用參數和加密等動態條件，以便系統可以支援其他方案，例如點對點通訊協定、計數及保險等。

然而，電子投票系統需要更多的周邊設備，而不是冗餘數據的創建和計數，身份驗證和憑證管理才是最關鍵的因素，通常機密性和真實性是附加的必備條件，並非所有皆可通過典型的以太坊系統獲得。另一方面，即使沒有中央機構的認證，也可以很好地支持完整性，而且由於所有條件和交易都是公開可用的，更透明的「白盒 (white box)」投票系統是可能的，但是在許多情況下會影響投票程序或系統的政治和社會經濟因素，應與技術可行性一起評估。

綜上，我們可以看到使用區塊鏈應用在電子投票和安全識別的巨大潛力，然而，技術和系統仍可能需一些時間才能成熟，但這天將指日可待。

七、更加安全的馬爾他 eID 和 ePASSPORT

馬爾他 (Malta) 是位在南歐地中海中心的一個島國，首都是瓦萊塔 (Valletta)，經濟來源以服務業和金融業為主，旅遊業是馬爾他主要的外匯來源。

近年來，馬爾他身份發行機構 (Identity Malta Agency) 透過推出新一代 eID 卡和 ePassport 來因應文件偽造和身份盜竊的全球性威脅，在符合國際安全標準的同時，採取更高階之防偽措施及防偽設計，使其更為出色。

(一) 馬爾他國民身份證 (National ID) 之沿革

馬爾他於 1975 年發行第一張身份證；1995 年發行第一張雷射列印身份證；2004 年馬爾他正式成為歐盟成員，發行可在歐盟申根國間旅行之身份證；2014 年大規模推出 E-ID；而在 2017 年發行之身份證明文件上有 X 標誌。

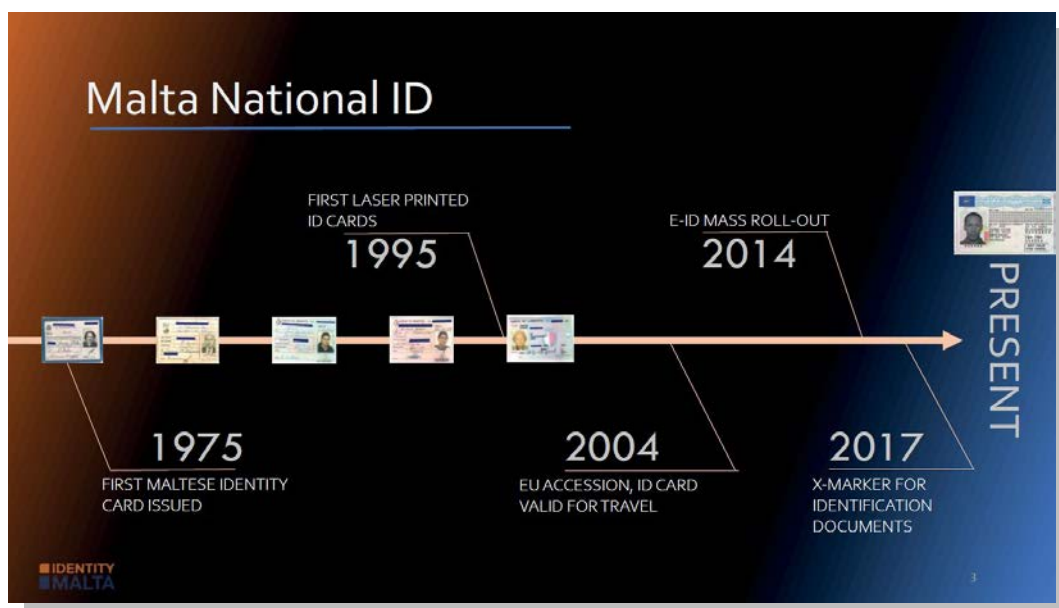


圖 4-7-1 馬爾他國民身份證（National ID）之發行歷史
（資料來源：2019 INTERGRAF Copenhagen proceedings）

（二）馬爾他面臨之挑戰及解決方案

馬爾他在身分證及護照等身分文件持續面臨仿製品、偽造及竄改等威脅。

1. 仿製品

- (1) 使用替代材料複製原版之仿製品。
- (2) 掃描原作文件，並使用電腦軟體進行修改。
- (3) 使用市售之層壓板、紙張和其他材料。

【解決方案】 設計一個難以複製，重製和個性化的檔案。

2. 偽造

欺詐者會更改身分文件中的有效資訊，包括：

- (1) 替換照片
- (2) 替換頁面
- (3) 更改個人資料（如以物理或化學方式擦除）

【解決方案】 (1) 使個人資料與強大的防偽功能結合，增加更改難度。

(2) 個人資料應為檔案一部分，而不僅僅是印在材料表面上。

3. 篡改

(1)使用無法正常運作的晶片，致檢測站無法讀取或驗證個人資訊。

(2)使用第二顆晶片產生假的個人資訊，偽裝為原來卡片上的晶片。

【解決方案】須提供在不破壞卡片的情況下，可以容易看出篡改跡象的卡片。

(三) 馬爾他的新安全功能

為解決上述威脅，馬爾他採用各先進國家身分文件所使用的聚碳酸酯 (Polycarbonate, PC) 材質做為新版身分證及護照之卡體，其特色為：

1. 聚碳酸酯是一種特殊材質，經過高溫和高壓下層壓，使各層材質熔融 (lamination) 為一體 (mono-block)，以致無法剝離，使證件幾乎無法被篡改，因此在不造成外觀明顯損壞的情況下，也不可能存取卡片中的防偽特徵和個人資料。
2. 雷射光打在可雷射蝕刻層 (Laser engravable transparent PC) 會產生碳黑化學反應，使表面形成黑色文字或圖像，主要用以產生個人化資料，可有效避免偽變造之情事發生。
3. 卡體經層壓熔融可產生凹凸觸感 (embossing)。
4. 非接觸式晶片 RFID (Radio Frequency Identification, 無線射頻識別技術) 係內嵌於卡體，故可支援所有防偽特徵功能，並維持卡片表面設計版面之完整性。
5. 平均使用壽命可達 10 年以上的耐用性。

(四) 新馬爾他晶片身分證 (eID) 之防偽功能

1. 卡體採用聚碳酸酯 (PC)
2. 透過雷射蝕刻產生個人化資料

3. 嵌入式防偽功能，各項防偽特徵如雷射蝕刻個人資料、浮凸壓紋、透明視窗及多重影像等，皆保存在卡體內部。
4. 採非接觸式單晶片之嵌入式 RFID 通訊，用於存取個人身份資料。
5. 正面防偽特徵（須於設計階段放入），包括：
 - (1)微小字（Micro Text）
 - (2)線條粗細變化（Line Modulation）
 - (3)嵌印式透明繞射光學變化影像裝置(Diffractive Optically Variable ImageDevices，DOVID)。
 - (4)扭索圖紋（Guilloche Pattern）
 - (5)光環圖紋（Aura Pattern）
 - (6)彩虹印刷（Rainbow Print）

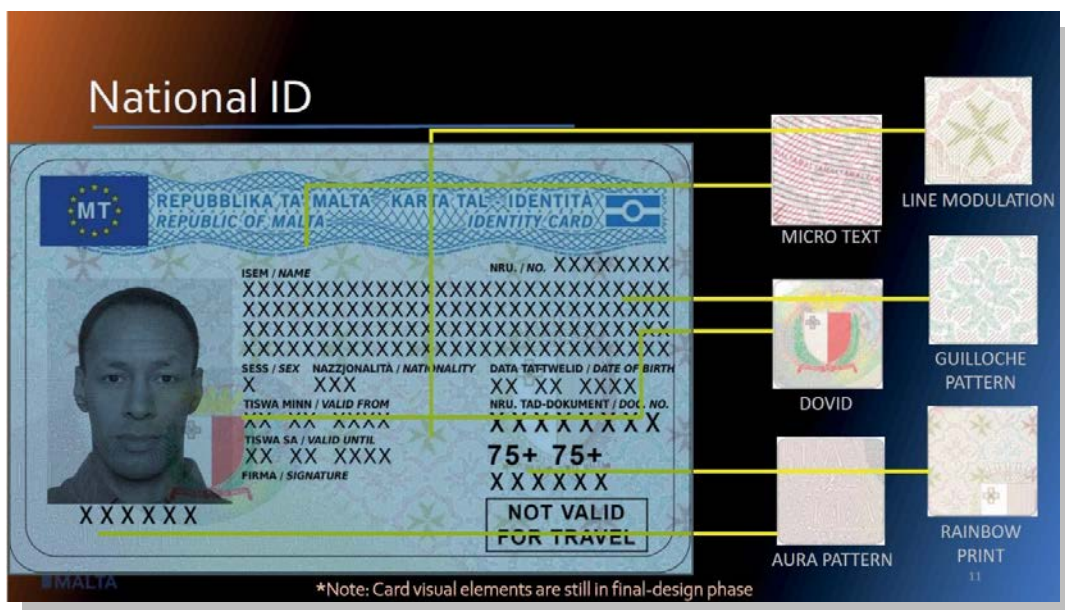


圖 4-7-2 馬爾他國民身份證正面之防偽特徵
 （資料來源：2019 INTERGRAF Copenhagen proceedings）

6. UV 防偽特徵

- (1)螢光油墨（Fluorescent Ink）
- (2)彩虹印刷隱性油墨（Rainbow Printed Invisible Ink）
- (3)隱形扭索圖紋（Invisible Guilloche Pattern）

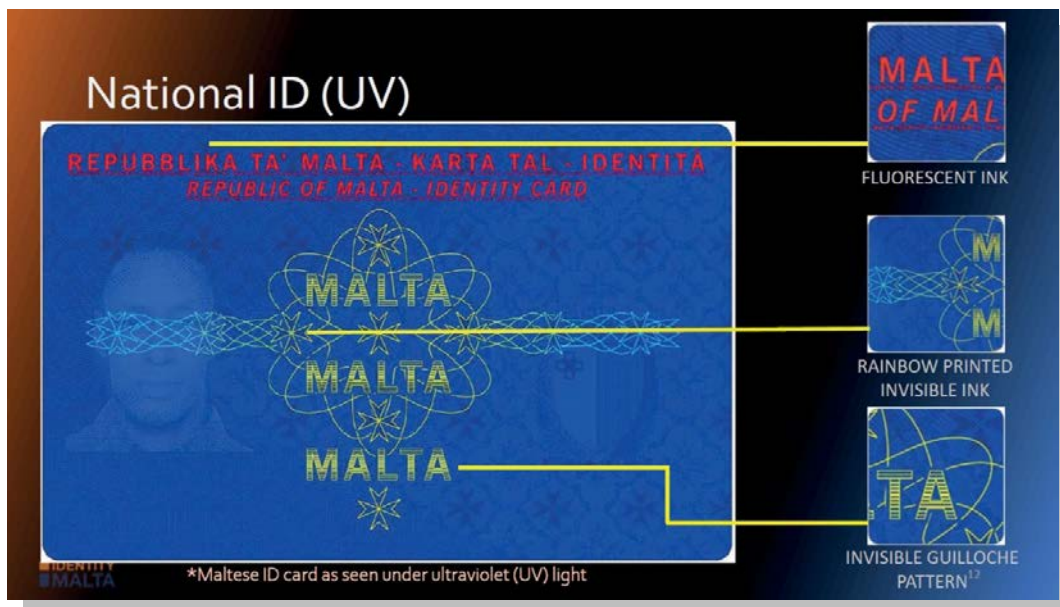


圖 4-7-3 紫外線 (UV) 光下之馬爾他身份證

(資料來源：2019 INTERGRAF Copenhagen proceedings)

7. 背面防偽特徵 (須於設計階段放入)，包括：

(1) 折光變色油墨 (Optically Variable Ink, OVI)

(2) 多重雷射影像 (Multiple Laser Image, MLI)，係卡面內嵌雷射影像或個人資訊，透過證卡表面之光柵 (濾鏡)，可隨觀察角度之轉變，產生不同繞射效果，進而呈現出不同影像。

(3) 個人之 QR code 識別號 (QR Code Identifier)

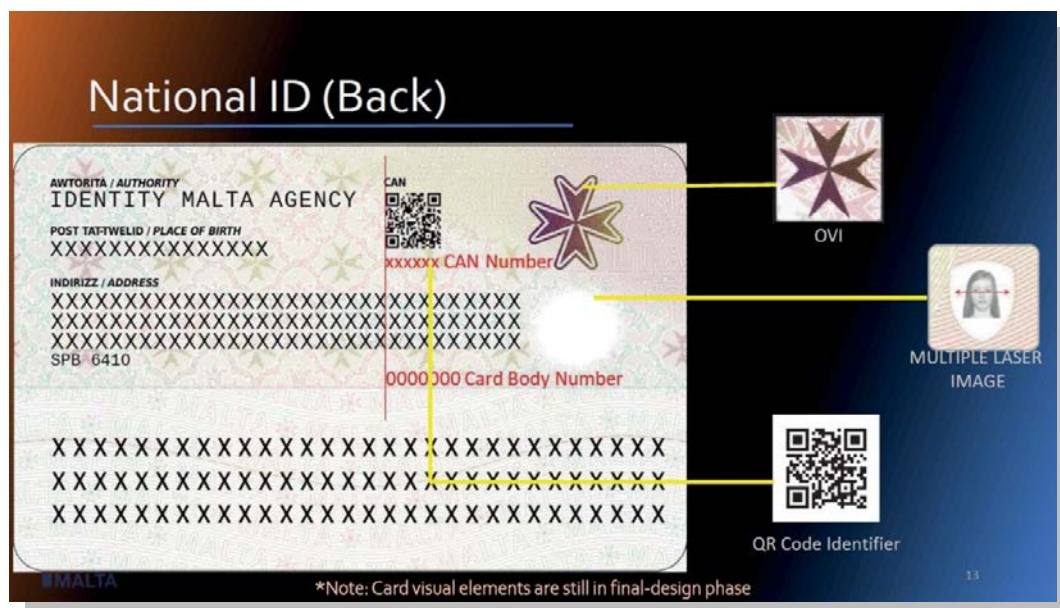


圖 4-7-4 馬爾他國民身份證背面之防偽特徵

(資料來源：2019 INTERGRAF Copenhagen proceedings)

(五) 新馬爾他晶片護照 (ePassport) 之防偽功能

馬爾他政府於 2019 年底前發行的 ePassport，除資料頁採用聚碳酸酯(PC)外，簽證頁則是採用含螢光纖維絲、浮水印及安全線等特徵之安全用紙，此外嵌入式晶片置入持照人之生物特徵，可用以查驗身份。

1. 護照資料頁採聚碳酸酯 (PC) BIO (個人生物特徵)，護照晶片內存儲持有人之基本資訊及持照人之生物特徵，如臉部特徵和指紋等，用以驗證旅行證件持有人的身分。
2. 透過雷射蝕刻產生個人化資料
3. 嵌入式防偽功能，各項防偽特徵如浮凸壓紋、透明視窗及多重影像等，皆保存在卡體內部。
4. 護照資料頁正面 (BIO-個人生物特徵)
 - (1)透明視窗 (Window)
 - (2)重雷射影像 (Multiple Laser Image, MLI)
 - (3)多重凹凸觸感特徵 (Several Tactile Embossing Features)

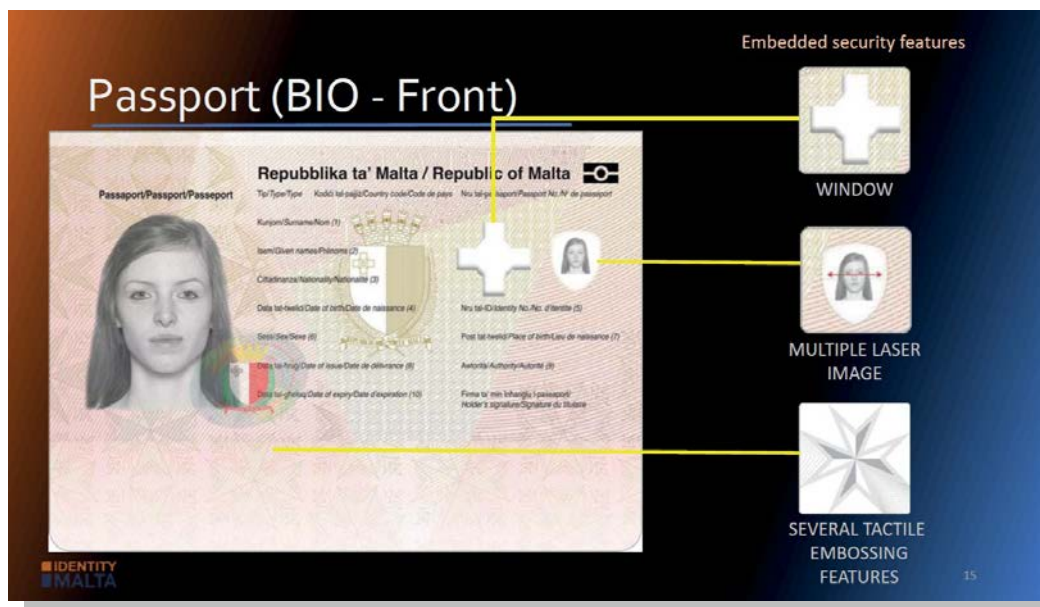


圖 4-7-5 馬爾他晶片護照正面之防偽特徵
(資料來源：2019 INTERGRAF Copenhagen proceedings)

5. 護照 (BIO-背面)

- (1)特殊網屏 (Bespoke Custom Screen)
- (2)線條粗細變化網屏 (Line Modulated Screen)
- (3)隱性圖紋彩虹印刷 (Invisible Rainbow Pring)
- (4)透明視窗 (Window)
- (5)光影變化箔膜 (OVI)
- (6)故意的錯誤 (Deliberate Error)
- (7)「REPUBBLIKA TA MALTA REPUBLIC OF MALTA」字樣以特小字體印刷 (Extra Small Print reading: REPUBBLIKA TA MALTA REPUBLIC OF MALTA)
- (8)彩虹印刷 (Rainbow Print)

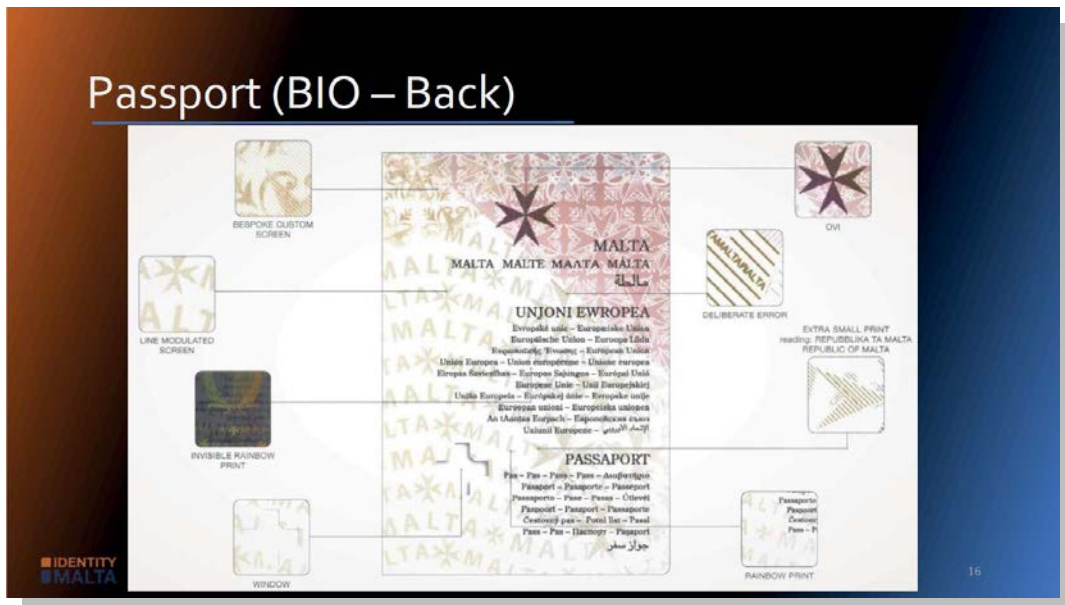


圖 4-7-6 馬爾他晶片護照背面之防偽特徵
(資料來源：2019 INTERGRAF Copenhagen proceedings)

6. 護照簽證內頁之防偽特徵

內頁印製馬爾他之著名地標和文化遺產等圖像，複雜之設計圖紋與防偽功能結合，並以須管制難以取得之防偽油墨印刷，其防偽特徵包括。

- (1)特殊網屏（Bespoke Custom Screen）
- (2)線條粗細變化網屏（Line Modulated Screen）
- (3)隱藏圖紋（Invisible Fan Feature）
- (4)頁碼整合以凹版印製（Intergrated Page Numbers）
- (5)隱性圖紋彩虹印刷（Invisible Rainbow Pring）
- (6)正反套印刷（See-Through Featruue）
- (7)彩虹印刷（Rainbow Print）
- (8)「MALTA」字樣以特小字體印刷(Extra Small Print and Remic reading: MALTA)
- (9)頁面主題以特殊網屏設計（User Definable Screen reading: Page Title）



圖 4-7-7 馬爾他晶片護照簽證內頁之防偽特徵
 （資料來源：2019 INTERGRAF Copenhagen proceedings）

八、ISO 14298 安全印刷流程管理認證

縱使現今防偽科技日新月異，全世界的安全文件仍面臨重大威脅，例如使用偽造身份證件和旅行證件非法越境、偽造貨幣進入全球流通市場，以及偽造出生證明以製造假身份等。為防止偽造情事不斷發生，鈔券和身份證件之防偽設計越來越精密與複雜，但偽造品亦是如此，因此如何掌握不斷快速發展的防偽科技，並大幅領先偽造者，是安全印刷業者不能停止的挑戰。

（一）ISO 14298 與 CWA 15374

此次國際安全印刷人會議主辦單位 INTERGRAF，為促進和保護安全印刷業者之利益，自 2001 年起結合 IHMA、UPU、VPGI，CEN 及歐盟委員會等來自世界各地的技術專家，依據國際標準規範，為安全印刷產業建立一套標準安全管理系統，並於 2003 年啟動認證計劃，確保安全印刷品的品質與服務，可以在完整的安全系統及風險管理下被穩定地生產，從而消除客戶及其產品的風險。

INTERGRAF 先於 2003 年推行適用於安全印刷業之「CWA 14641 防偽印刷安全管理系統」，又於 2005 年推行適用於安全印刷軟硬體、設備及原物料供應商之「CWA 15374 安全管理系統」，確保安全印刷業者及其供應商的產品從開發到印刷之最大安全性，建立上下游供應鏈之安全防護，進而消除客戶及產品的風險。而 CWA 14641：2009 版本於 2013 年升級為 ISO 14298：2013，原有的 CWA 14641：2009 證書自 2016 年 12 月 31 日起失效。

對歐洲國家而言，ISO 14298 和 CWA 15374 認證已成為具信任與品質之保證，例如歐洲議會（European Parliament）和歐洲理事會（European Council）在其法規中均引用 INTERGRAF 的 ISO 14298 做為「簽證文件（歐盟）2017/1370」及「第三國國民居留許可證（歐盟）2017/1954」之統一格式。

1. ISO 14298：2013 安全印刷流程管理

ISO 14298 主要針對安全印刷業者、全息圖（hologram）製造商及有價證件的業者，及其所生產製造之鈔券、身份證、護照、駕駛證、防止偽造許可證、郵資和稅票、全息圖及證書等產品的生產流程，從設計圖檔、印刷生產過程及最後廢棄物的銷毀，所有過程及數量皆可完全持續地被控制，以防安全印刷品被偽造。



圖 4-8-1 ISO14298 認證

ISO 14298 的認證等級（Certification levels）分為以下 3 種：

- (1) **FUNDAMENTAL**：適用於為非政府組織和政府組織提供商業安全印刷品和安全產品之安全印刷業者。
- (2) **GOVERNMENTAL**：適用於為政府提供商業安全印刷產品和安全產品（包括身份證件及護照等）之安全印刷業者。
- (3) **CENTRAL BANK**：適用於為中央銀行或信用卡發行機構提供服務的安全印刷業者，以及身份證及護照之個人化中心。

公司必須滿足相應級別之任何要求，才能獲得相關級別的證書。同一建築內生產的所有產品必須符合相關標準，並在同一級別下運行。

2. CWA 15374：2018 安全管理系統

CWA 15374 是規範防偽功能產品和服務之供應商，以確保提供給安全印刷業者使用的原物料（如油墨、證券紙、層壓板、安全箔、鑲嵌物、安全設計軟體、基材、顏料、塗料及機械設備等）符合安全標準。



圖 4-8-2 CWA 15374 認證

（二）通過認證之效益

通過認證方案具有許多好處，先是從客觀和外部角度對公司進行評估，有助於發現薄弱環節和運營盲點，以提升競爭力，還包括以下效益：

1. 可經考驗的安全管理系統
2. 從開發到部署的最大安全性
3. 明確的需求和責任結構
4. 防止和打擊偽造和變造
5. 受信任的安全印表機或供應商
6. 政府和業界公認之參考
7. 提高客戶信心和滿意度



圖 4-8-3 INTERGRAF 認證效益圖
 (資料來源：www.securityprinters.org)

(三) 如何取得認證

1. ISO 14298 還是 CWA 15374 ?

INTERGRAF 會根據需求，協助選擇最適合公司之認證標準。

2. 詢問

向 certification@INTERGRAF.eu 索取申請表。

3. 申請

向 INTERGRAF 提交申請書，並附上所有隨附的文件。

4. 《INTERGRAF 認證要求》和《實施指南》

所有申請公司皆須經篩選後，才能收到 INTERGRAF 之機密認證要求。如果不符合要求之條件，INTERGRAF 得以保留拒絕申請之權利。若得到肯定之評估，INTERGRAF 將發送《INTERGRAF 認證要求 (INTERGRAF Certification Requirements, ICR)》和《實施指南 (Implementation Guidelines)》，幫助公司進行差距分析，然後安排公司選擇之認證機構進行審核。

5. 預評審核

為避免營運和流程中的差距可能會延誤認證，公司可選擇是否進行初步檢查，以便更完善地為認證審核做準備。

6. 認證審核

認證機構會評估公司是否成功地遵守 INTERGRAF 認證要求 (ICR)，並向 INTERGRAF 發送審核報告。

7. 認證

一旦認證機構確認公司之操作和生產製程沒有不合格項目，INTERGRAF 將會簽發一份正式證書，明確說明公司的認證範圍，並在 www.securityprinters.org 上列出。

(四) INTERGRAF 認證要求 (ICR) 與實施指南

顧及安全印刷產業全球市場之特殊需求，INTERGRAF 針對該產業制定《INTERGRAF 認證要求 (INTERGRAF Certification Requirements, ICR)》與《實施指南 (Implementation Guidelines)》，詳細描述從訂單到最終交付過程中必須採取之安全措施。《INTERGRAF 認證要求 (ICR)》有 69 頁、13 個章節、99 個項目，可作為檢查表，用以確認公司之規範及流程是否滿足認證之要求。由於包含機密訊息，故為非公開文件，僅提供給認證申請已被 INTERGRAF 積極審查之公司。通過認證後，每年都要持續進行審核和更新，以確保達到最高的質量標準。

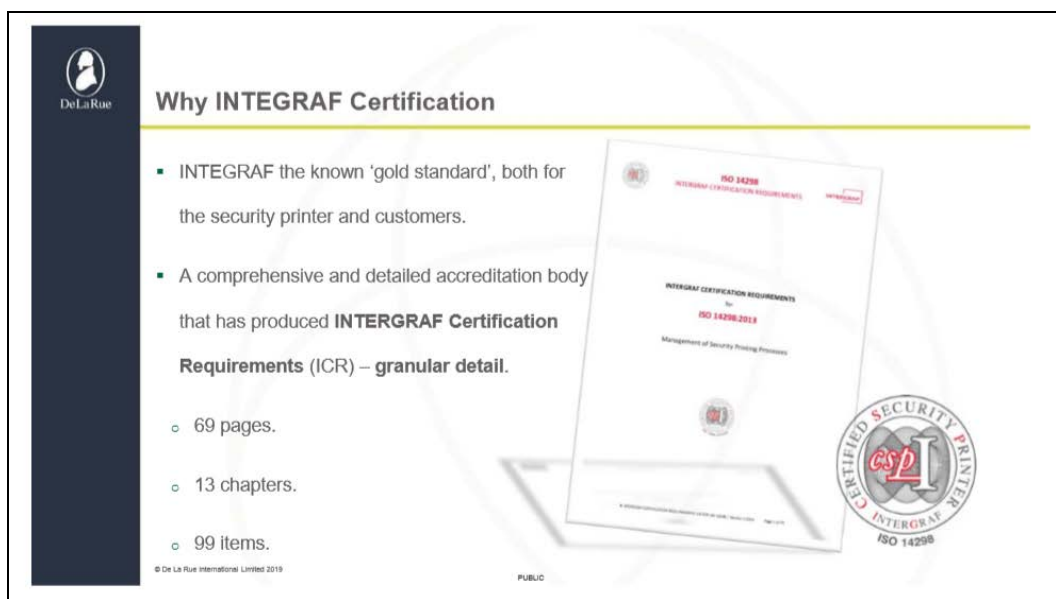


圖 4-8-4 《INTERGRAF 認證要求 (ICR)》細節
(資料來源：2019 INTERGRAF Copenhagen proceedings)

(五) 預評審核 (Pre-assessment audit)

為確保審核進行順利，公司在進行認證審核前，可先選擇是否在實際現場進行預評審核，目的是評估公司目前的管理系統是否符合 ISO 14298 或 CWA 15374 之標準。過程中，審計師會先審查所有文件、檔案及生產流程，與流程負責人面談，並評估實體和邏輯之安全性，針對認證過程狀態及調查結果歸納成一份客觀概述的報告，提供廣泛而全面的資訊，這可以幫助公司實施糾正措施，節省不必要的成本和工作量。

(六) 認證審核 (Certification audit)

一旦公司決定繼續進行認證，認證機構便會開始進行認證審核，協助解決弱點並實施《INTERGRAF 認證要求 (ICR)》。審核員會有幾天待在現場，對管理體系的實施和運行情況進行稽核，認證機構會將所有發現的結果匯總於綜合報告中，以便專注於需要改進的關鍵領域和流程。認證機構會根據客觀證據進行判定，不合格通常有兩種類型：嚴重不合格（基於缺乏和/或維持，

不遵守標準和《INTERGRAF 認證要求》的重大或系統性失敗)和輕微不合格(管理系統的弱點,或可能導致嚴重不合格的小問題)。

認證機構做出肯定的認證決定後,INTERGRAF 將會發送最終審核報告並頒發證書,證書有效期為三年。然而,認證是一個長期持續改進的專案,每年必須進行年度控制稽核,以確保公司能持續遵守標準、政策和流程,並在第二年進行第一次控制稽核,然後在第三年進行第二次控制稽核,三年後,則必須重新進行認證審核。定期的控制稽核和《INTERGRAF 認證要求(ICR)》的年度更新,可確保持續的高安全性,而每三年認證週期內的定期審查和重新評估,則有助於不斷提高其有效性。

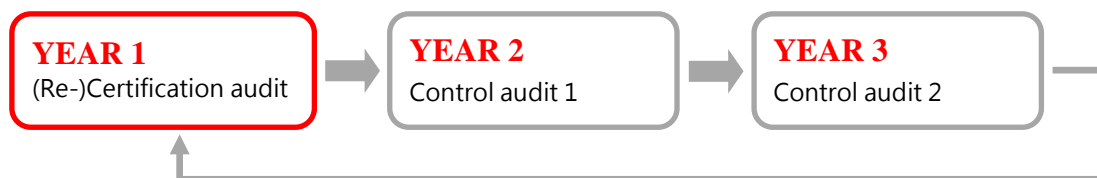


圖 4-8-5 INTERGRAF 認證週期圖

(資料來源：2019 INTERGRAF Copenhagen proceedings)

(七) 培訓 (Training)

INTERGRAF 為已通過 ISO 14298 和 CWA 15374 認證的公司,以及希望獲得認證的公司定期舉辦研討會及培訓課程,重點是安全印刷管理系統的實施和維護,涵蓋的主題範圍包括:

1. 差距分析
2. 內部稽核流程
3. 改進內部之流程與效率
4. ISO 管理系統標準的高階結構(HLS)之效益
5. 資訊安全
6. 員工在工作場所的意識和積極態度

(八) 認證費用

認證費用取決於公司之規模與運營地點數量（詳表 4-7-1 和表 4-7-2），

費用包含 2 種：

1. 由 INTERGRAF 開具管理費發票：對於隸屬於 INTERGRAF 的歐洲國家印刷聯合會的成員，適用於特殊條件。
2. 由認證機構開具與審核相關的費用發票：旅行和住宿費用將單獨開具發票，所有價格均為歐元，不含增值稅。

表 4-8-1 ISO 14298 認證費用明細表

單位：歐元

費用內容		年 度		
		第一年 稽核費用	第二年 稽核費用	第三年 稽核費用
由 INTERGRAF 收取之費用	行政管理費－主場地	4,000	800	800
	行政管理費－附加場地	每個場地 + 600	每個場地 +800	每個場地 +800
	認證書副本	150	-	-
由 認證機構 收取之費用	有 1~40 名員工公司 之查核費用	3,555	2,962	2,962
	有 41~100 名員工公司 之查核費用	4,740	3,555	3,555
	有 101~500 名員工公司 之查核費用	5,925	4,148	4,148
	有 500 名以上員工公司 之查核費用	7,110	4,740	4,740

（資料來源：2019 INTERGRAF Copenhagen proceedings）

表 4-8-2 CWA 15374 認證費用明細表

單位：歐元

年 度		第一年	第二年	第三年
費用內容		稽核費用	稽核費用	稽核費用
由 INTERGRAF 收取之費用	行政管理費－主場地	3,000	600	600
	行政管理費－附加場地	每個場地 + 600	每個場地 + 600	每個場地 + 600
	認證書副本	150	-	-
由 認證機構 收取之費用	有 1~40 名員工公司 之查核費用	3,555	2,962	2,962
	有 41~100 名員工公司 之查核費用	4,740	3,555	3,555
	有 101~500 名員工公司 之查核費用	5,925	4,148	4,148
	有 500 名以上員工公司 之查核費用	7,110	4,740	4,740

(資料來源：2019 INTERGRAF Copenhagen proceedings)

(九) 客戶的觀點——De La Rue

本次會議 De La Rue 也以客戶的觀點分享為什麼選擇 INTERGRAF 認證的原因。De La Rue 位於全球的分公司中，有 7 家分別取得 CWA 15374 與 ISO 14298 認證（詳表 4-8-3）。

De La Rue 認為，INTERGRAF 認證不是建立一套複雜且難以管理的程序，而是提供一種實用且可行的管理系統和實施細節，用以改善和監控生產流程中有關風險的部分，為生產流程和供應鏈奠定堅實的基礎，建立強大的安全基準，使整體的安全環境達到「黃金標準（gold standard）」，以因應客戶日益增加的需求，進而提高客戶對產品之滿意度和信心，企業利潤也能因此增加。

表 4-8-3 De La Rue 通過認證之分公司

公司名稱	所在地	取得年度	認證種類/等級
1 PORTALS DE LA RUE LIMITED – Bathford	英國	2014 年	CWA 15374
2 PORTALS DE LA RUE LIMITED – Overton	英國	2014 年	CWA 15374
3 De La Rue Currency and Security Print Limited	肯亞	2014 年	ISO 14298 Central Bank level
4 De La Rue International Ltd.	英國	2015 年	ISO 14298 Governmental level
5 De La Rue Lanka Currency & Security Print (Pvt.) Ltd.	斯里蘭卡	2016 年	ISO 14298 Central Bank level
6 De La Rue Currency & Security Print Ltd, Supply Chain Malta	馬爾他	2016 年	ISO 14298 Central Bank level
7 De La Rue International Ltd.	英國	2019 年	ISO 14298 Central Bank level

(資料來源：www.securityprinters.org)

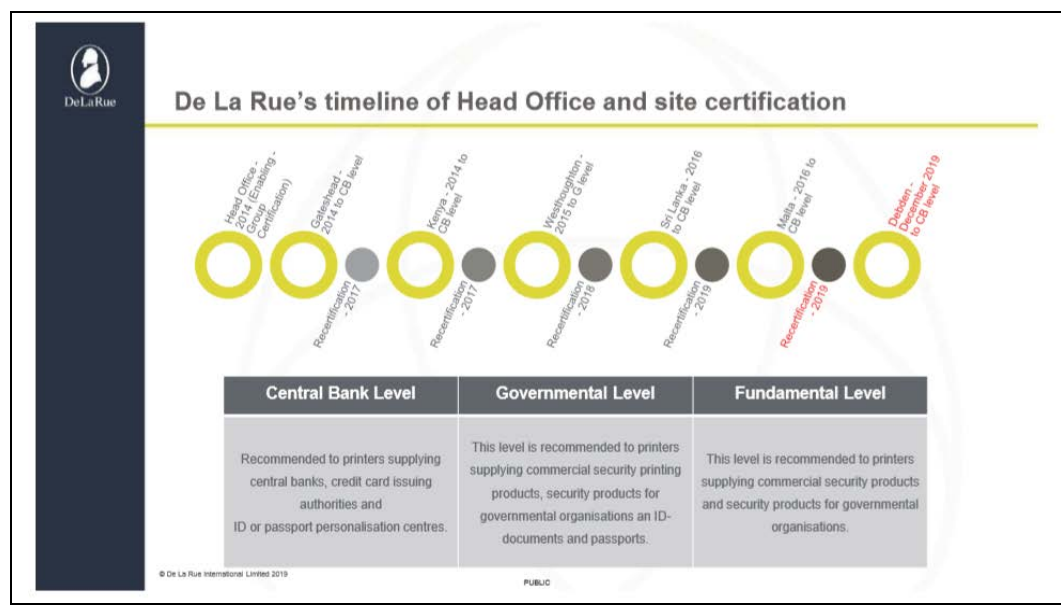


圖 4-8-6 De La Rue 總部和其他現場通過 ISO 14298 之時間表

(資料來源：2019 INTERGRAF Copenhagen proceedings)

(十) 全球與臺灣通過認證現況

截至 2019 年 12 月底為止，全世界已有 145 家公司取得 ISO 14298 與 CWA 15374 認證，遍布五大洲的 53 個國家／地區。有 128 家安全印刷業者取得 ISO 14298 認證，其中取得 Fundamental level 的公司有 31 家，取得 Governmental level 的公司有 65 家，而取得 Central Bank level 的公司有 32 家，主要為國家印鈔廠或協助他國印製鈔券或身份文件的公司，如 De La Rue 和 Gemalto 等。

表 4-8-4 全世界取得 ISO 14298 及 CWA 15374 認證之等級及公司家數

認證種類 認證等級	ISO 14298	CWA 15374
Fundamental level	31 家	17 家
Governmental level	65 家	
Central Bank level	32 家	
合計	128 家	17 家

(資料來源：www.securityprinters.org；本報告整理)

另有 17 家世界知名供應商取得 CWA 15374 認證，包括 OVD Kinegram AG、IDEMIA France SAS、Veridos Matsoukis Security Printing S.A. Mühlbauer GmbH & Co. KG 及 HID Global CID 等。

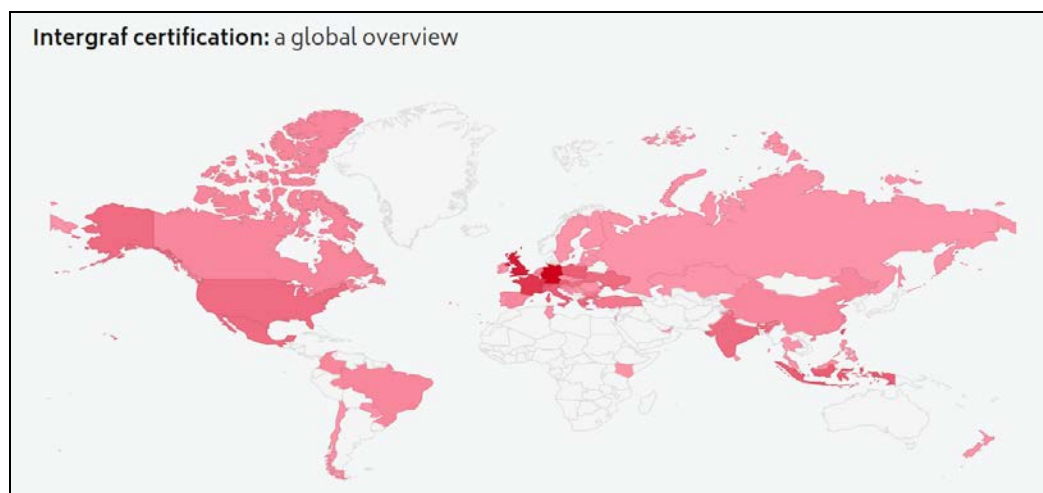


圖 4-8-7 全球 INTERGRAF 認證概覽

(資料來源：www.securityprinters.org)

由圖 4-8-7 和表 4-8-5 可得知，取得 ISO 14298 及 CWA 15374 認證的國家，主要仍集中在歐洲，其次為亞洲、美洲、澳洲及非洲。

表 4-8-5 全世界取得 ISO 14298 及 CWA 15374 認證之國家與公司家數

洲別	國家數	公司家數	備註
歐洲	28 國	88 家	德國(12 家)、英國(10 家)、法國(8 家)、義大利(6 家)、瑞士聯邦(6 家)、匈牙利(5 家)、波蘭(5 家)、希臘(4 家)、烏克蘭(4 家)、保加利亞(3 家)、比利時(2 家)、捷克(2 家)、立陶宛(2 家)、馬爾他(2 家)、斯洛維尼亞(2 家)、西班牙(2 家)、荷蘭(2 家)、波士尼亞與赫塞哥維納(1 家)、克羅埃西亞(1 家)、愛沙尼亞(1 家)、芬蘭(1 家)、愛爾蘭(1 家)、拉脫維亞(1 家)、葡萄牙(1 家)、羅馬尼亞(1 家)、俄羅斯(1 家)、塞爾維亞(1 家)、瑞典(1 家)
亞洲	14 國	32 家	臺灣(7 家)、印尼(5 家)、印度(4 家)、中國(3 家)、土耳其(3 家)、阿拉伯聯合大公國(2 家)、香港(1 家)、以色列(1 家)、哈薩克(1 家)、馬來西亞(1 家)、菲律賓(1 家)、新加坡(1 家)、斯里蘭卡(1 家)、泰國(1 家)
美洲	7 國	17 家	墨西哥(5 家)、美國(4 家)、巴西(2 家)、加拿大(2 家)、哥倫比亞(2 家)、智利(1 家)、巴拉圭(1 家)
澳洲	2 國	6 家	澳大利亞(5 家)、紐西蘭(1 家)
非洲	2 國	2 家	肯亞(1 家)、突尼西亞(1 家)
合計	53 國	145 家	

(資料來源：www.securityprinters.org；本報告整理)

值得注意的是，台灣有 7 家公司取得 ISO 14298 認證，為亞洲國家中最多者，其中有 5 家為 Fundamental level，另有 2 家為 Governmental level (見表 4-8-6)，主要承製郵票、塑膠證卡、有價證券及防偽標籤等產品。

表 4-8-6 台灣取得 ISO 14298 認證之公司

公司名稱		產品項目	認證等級
1	卡登實業股份有限公司 CARDON ENTERPRISE CO., LTD	郵票、塑膠證卡及有價證券	Fundamental level
2	中華彩色印刷股份有限公司 China Color Printing Co., Ltd.	郵票及有價證券	
3	鉅冠印刷股份有限公司 Jiuh Guan Security Printing Co Ltd	有價證券	
4	台灣銘板股份有限公司 Taiwan Name Plate Co. Ltd.	塑膠證卡	
5	永豐紙業股份有限公司 Yuen Foong Paper Co Ltd	有價證券及防偽標籤	
6	第一美卡事業股份有限公司 Beautiful Card Corporation	塑膠證卡	Governmental level
7	宏通數碼科技股份有限公司 Foongtone Technology Co., Ltd.	塑膠證卡	

(資料來源：www.securityprinters.org；各公司網站)

伍、心得與建議

感謝長官指派職等兩人參與此次安全印刷產業之國際年度盛會，實深感榮幸，過程中除獲取許多與安全印刷相關新科技與新觀念外，更在會中與來自各國之專業人士針對案例研究及實務經驗進行交流，深具啟發且受益良多，謹提出以下淺薄之見，以期對本廠有所助益。

一、持續派員參加相關國際會議

目前科技日新月異，3C 商品愈發普及且價錢也越來越低廉，不再需要特別高的價錢或是特別的通路都能取得高解析度的掃描器和印表機，這也意味著偽造鈔券及安全文件的門檻越來越低，因此傳統的防偽方式已不足以對抗，需仰賴複合式的防偽方法或是新式的印刷材質、油墨等新式防偽科技來阻擋偽造或是變造，為達此目標，建議能持續派員參加相關國際會議，將最尖端之防偽科技新知帶回本廠與同仁共同研討，使本廠技術能夠向前邁進。

二、進行各式軟硬體設備更新準備

隨著目前科技發展日新月異，安全印刷的各相關軟硬體設備也不斷推陳出新，目前中央印製廠之主力印刷及檢查機器設備多已使用數十載，建議可逐年更新或導入新式軟、硬體設備。

搭配新機器設備之使用，人力需求也將由勞力方面的需求轉為技術性操作需求，對於現場人員來說也能節省時間、體力並避免發生工作傷害的機會；在鈔券設計方面，新一代的安全印刷設計軟體搭載之功能亦可增加設計製作效率以及減少錯誤發生機率，目前本廠已採購並使用新版設計軟體，根據使用之人員反應及使用測試成效良好，建議將來亦持續關注軟體更新消息，評估其使用導入是否可再提升效益。

另參考他國改版經驗，若使用複合式紙張或是塗佈之棉紙印製鈔券可有效提升鈔券之使用壽命。本廠近年來亦積極嘗試塑膠鈔券或是複合材質之鈔券打

樣，建議對於打樣成果除觀察視覺效果呈現外，亦可加上測試其耐流通性，若其使用壽命顯著高於現行使用的棉紙基材，將來在改版時亦可納入採用之考慮。

三、加強員工資訊訓練

目前各種新式印刷機越來越倚重電腦以及自動控制的部分，而各國在鈔券識別輔助或是推廣方面亦是藉由 APP 軟體達成，故資訊能力已是無法忽視的趨勢，建議將來能提供更多資訊訓練予員工，提升員工資訊能力，進而有更好的工作達成率。

四、及早投入護照 PC 資料頁之研發與規劃

美國新版護照預計於 2020 年發行，其資料頁係採用聚碳酸酯(polycarbonate, PC) 材質，而我國護照製作一向依循美國護照之規格，因此護照改版將有可能在近幾年內發生。聚碳酸酯材質為目前各國身分文件採用之趨勢，相較於護照專用紙張，其印刷、熔融、模切與裝訂等製程與相關參數設定皆為新挑戰，因此，為及早因應局勢變化及客戶需求，本廠應儘速積極投入護照 PC 資料頁之防偽設計與生產技術研發，以及相關生產設備之市場調查與規劃，有備無患。