內政部

新一代國民身分證換發規劃案

規劃成果重點報告

中華民國 109 年 11 月

目錄

表目錄

圖目錄

第壹章、背景說明

查戶籍法第 52 條規定：「國民身分證及戶口名簿之格式、內容、繳交之相片規格，由中央主管機關定之。(第 1 項)國民身分證及戶口名簿之製發、相片影像檔建置之內容、保管、利用、查驗及其他應遵行事項之辦法，由中央主管機關定之。(第 2 項)」有關國民身分證「格式」係指證卡規格樣式，舉凡證卡材質、尺寸大小、雙頁折疊式或單頁式、男女分色等均屬之；至國民身分證「內容」，係指所記載之資料，隨著時空背景不同，歷來國民身分證所載內容亦不斷變化，例如過去曾載有指紋符號、職業、血型、教育程度等。因應時代演變，強化個資及隱私保護，並配合資通訊科技技術及強化卡片防偽需求，諸多證卡均改以「晶片式」格式，如政府機關核發之健保卡、晶片護照、居留證，以及私部門發行之金融卡、信用卡等，晶片式製卡已成為發展趨勢，而國民身分證納入「晶片」之議題，僅涉及國民身分證「格式」與所載「內容」之調整，依戶籍法第 52 條之規定，均已授權由中央主管機關定之。

我國國民身分證制度自 36 年實施以來，已融入社會大眾生活，為國人最基礎且重要的身分證件，自上次(94 年)全面換發迄今已逾 14 年，十幾年來因相貌改變，戶政機關留存的相片與本人實際相貌已有不同，不易精準確認人別，且現行國民身分證防偽安全雖有一定強度，但近來不法之徒鑽研偽變造手法日益精細，坊間已出現數宗幾可亂真之偽變造國民身分證案件，嚴重影響民眾身分財產及交易安全；隨著資通訊科技快速發展，電子化及數位化已成為全球趨勢，數位發展已為各國重要戰略之一，因此，加速數位轉型與提升數位治理競爭力，並提供人民更便利的生活，是政府刻不容緩之要務。考量現行國家數位發展需要，且為保障國民權益，借鏡多數國家發行晶片身分證明文件經驗，規劃全面換發國民身分證，除強化國民身分證用於面對面身分識別中的防偽措施外，又因應數位化趨勢，將網路身分識別功能納入國民身分證。網路身分識別目前有自然人憑證、全民健保卡等，其中以自然人憑證在身分識別強度最高且較廣泛，具電子簽章之不可否認性，可普及推行至所有人，爰以自然人憑證作為國民網路身分識別之首選。

保障個人隱私及降低資安風險是新式國民身分證(下稱New eID)規劃的首要原則,本部自102年起即針對國民身分證及自然人憑證之結合進行研究,104年起開始規劃換證工作,於104年10月擬具「晶片國民身分證全面換發計畫」(草案)報院,當年規劃採多卡合一方案(國民身分證結合自然人憑證、健保卡、保留電子票證區域),經國家發展委員會審議,應單純化晶片身分證之功能,爰遵循該原則展開研究,並蒐集各方意見,與民溝通,105年1月運用國家發展委員會「公共政策網路參與平台」廣徵民眾對於晶片國民身分證規劃構想、106年5月23日至11月22日辦理1場晶片國民身分證國際研討會、2場焦點團體座談會、1場工作坊及1次電話民調等與民溝通之開放決策活動(可參閱本部戶政司全球資訊網「New eID資訊公開專區」),復為完善換證作業,於106年起與相關機關、專家學者(電子治理、資安、法律)組成「晶片國民身分證換發專案工作小組」,研議New eID換發計畫及相關工作,並審核規劃妥適性。

107年10月17日國家發展委員會邀請本部報告國民身分證換發計畫,換發規劃之原則為單純晶片身分證功能,即僅將國民身分證附加自然人憑證。嗣國家發展委員會於107年12月27日行政院第3632次會議發表「智慧政府發展藍圖」,揭示數位身分識別證(New eID)是智慧政府基礎架構,經行政院院會決議請本部妥善規劃全面換發相關工作,於2020年啟動全面換發作業。

國家發展委員會所規劃之智慧政府,其二大基礎建設為普發New eID作為各機關服務的身分識別及建立具安全且可信賴的T-Road,作為各機關溝通的橋樑,因各資料庫仍由各機關自行管理維護,且使用New eID於網路作身分識別,係以自然人憑證為之,網路識別身分後,由各機關之服務程式將民眾所需之資料提供予該民眾,尚非指民眾可以使用New eID進入各機關資料庫恣意取用資料,此係兼顧資訊安全及分散風險之作法。

為打造智慧政府藍圖之New eID,爰於108年1月起展開各項換發New eID整備工作,先循行政程序提出換證計畫並匡列所需換證經費,於108年1

月 31 日將「數位身分識別證（New eID）—新一代國民身分證換發計畫」報院審議，復依行政院 108 年 3 月 15 日審議意見，於 108 年 3 月 26 日修正計畫再次函報行政院，經行政院 108 年 6 月 6 日函復原則同意；復為推動及完善全面換證計畫之各項工作，於 108 年 2 月 13 日擴大原工作小組規模、邀請更多專家學者擔任委員並更名為「新一代國民身分證換發工作小組」，其中工作小組之委員名單中包含數位資安學者專家，與會者之各項建議均予研議，並適度採納作為後續系統建置及各項作業執行之參考。自 108 年 3 月 25 日至 109 年 6 月 8 日已召開 5 次會議研商各項作業事宜。

New eID 之規劃採用多層加壓熱融合 PC 材質的晶片卡，其晶片電子防偽機制，可防止資料被竄改及複製，且卡面資訊最小化，並由民眾選擇是否附加自然人憑證，尊重資訊自主權利，若有附加自然人憑證，因具公開金鑰基礎建設（PKI）及電子簽章，可使用其自然人憑證作網路上的身分識別、簽章與資料保護，晶片內個資採分區存放並以密碼保護，公開區資料之讀取碼為卡片序號，一旦證件更換，讀取碼就不同，以保障民眾個資；此外，加密區及自然人憑證區，均須由本人親自設定 2 組不同長度之密碼，且該 2 區僅能插卡使用，不能感應讀取，強化晶片使用信賴度及安全強度，公開區及加密區只用在臨櫃面對面的身分識別及資料驗證，以及網路的資料驗證，不得單獨作為網路身分識別及簽章，須配套其他機制，如需簽章則要當事人親簽文件才可。

New eID 無論採用插卡及感應方式讀取資料，皆需通過晶片授權驗證，以感應方式讀取者，距離限於數釐米內且要輸入讀取碼才能讀取，綜觀各國 eID 的發展趨勢，讀取方式皆由插卡移轉至雙介面或感應，目前金融卡、信用卡也都支援感應讀取，其安全性也已經過國外長期驗證。

依戶籍法第 51 條國民身分證用以辨識個人身分，其效用及於全國，發行 New eID 之運用情境，由各機關依個別法令決定須臨櫃親辦或線上服務項目，如戶籍法第 33 條規定結婚登記以雙方當事人為申請人、土地登記規則第 40 條規定不動產移轉之登記義務人應親自到場，提出國民身分證正本、金融機構

防制洗錢辦法第 3 條規定金融業務受理開戶時，應實施雙重身分證明文件查核及留存該身分證文件，這些業務未來仍需親辦，至於線上服務，仍同現行使用自然人憑證作業方式，由各服務機關自行決定所提供之服務是否使用 New eID，以目前應用自然人憑證開發的 4,000 多項功能及 200 多項資訊系統，於使用自然人憑證作網路上的身分識別時，不會連回憑證中心，自然不會留下任何紀錄，又晶片已存有個人身分基本資料，也無須連回本部取用個資，且使用紀錄均留存在提供服務的機關(構)內部，只有民眾才知道使用歷程，本部無法知悉，無數位足跡被政府掌握及監控的疑慮。

考量數位落差情形，當民眾沒有網路、讀卡設備或不會使用網路服務時，仍可臨櫃辦理相關業務，並無強迫民眾使用電子化服務。民眾如不願意提供 New eID 予需用機關(構)讀取，也可向戶政事務所或上網申請晶片資料清單（具浮水印、騎縫章及檢查號碼供查驗資料內容有無被竄改，同現行電子戶籍謄本），再臨櫃辦理相關業務作為佐證資料。

New eID 換發之整體工作有製卡面、系統面、法規面、行政面、宣導面等均由本部統籌，各面向之作業可併行不悖，相關辦理情形如下：

一、 製卡面

考量卡片防偽、秘密諮詢、專屬權利、場域安全等因素，並參考其他國家，如德國、法國亦基於安全考量，選擇國家級印製廠進行，爰本部依政府採購法第 22 條第 1 項第 2 款規定，採限制性招標，委由百分之百國營的中央印製廠承製，整體製程均有層層安全管控檢測、製卡、專人保全運送至戶政作業單位。

另中央印製廠為完成本部委託之印製作業，須建置安全之廠域環境、進行相關材料及印製設備採購，為協助其準備招標製卡規格規範文件，細部規劃案廠商即提供卡片含晶片規格及需求、製卡中心規格、管理規範及安全規劃、製發管理規劃相關細部規劃案階段性成果予中央印製廠參採，本部並邀其共同參加細部規劃案會議，中央印製廠並於 108 年 8 月至 9 月進行對外公告 PC 晶

片卡及製卡設備招標規格之公開閱覽蒐集各界意見及舉辦說明會等前置作業，並於109年2月21日完成招標簽約。

借鏡愛沙尼亞eID之資安事件經驗，規劃New eID採雙晶片備援機制，確保晶片供應不致短缺，若遇晶片品質不符流通使用需求或有安全疑慮時，可及時啟動備援晶片。此外，亦設有雙金鑰備援方案，定期進行金鑰風險評估，依評估結果進行必要因應措施，確保晶片安全與個資隱私外洩風險降至最低；晶圓由台積電公司代工生產，晶片於新加坡封裝，均通過國際安全認證標準CC認證(Common Criteria)，且晶片之多項功能達安全評估等級EAL(Evaluation Assurance Level) 5+以上，已屬軍事機密等級，且要求至少要有千萬張的晶片卡須在臺灣生產製造，透過國際廠商技術移轉，提升國內產業技術。

二、 系統面

依政府採購法規定辦理New eID之各項招標案，且依規定過濾投標廠商資格，不允許大陸地區廠商、第三地區含陸資成分廠商及在臺陸資廠商參與，以符招標程序規定。

基於研析晶片身分證已數載，對於New eID之卡片採PC材質塑膠卡、彩色相片、個人資料採雷射雕刻、晶片容量及採雙介面、晶片內容分區及密碼控管讀取等，已有既定之原則方向。為謹慎及順利推動換發工作，及周延完備換證作業流程、資安規範、SOP等具體細節，乃再循一般資訊系統建置開發作業模式，先行辦理規劃案，於108年4月11日至11月30日委託國巨顧問管理公司辦理細部規劃，其報告書共10冊，為審慎計，均邀請專家學者召開審查會議協助審查，以完備報告書品質。

New eID系統面之建置工作，經參考細部規劃之建議，並納入國安會、行政院資安處及各界意見妥為修正「新一代國民身分證換發系統建置及維護案」招標文件，分別於108年11月29日至12月3日辦理第1次公開閱覽、108年12月18日至12月23日辦理第2次公開閱覽以蒐集各界意見，同時再將招標文件提請109年1月2日召開「新一代國民身分證換發系統建置及維護

案」採購評選委員會第 1 次會議討論修正後，於 109 年 1 月 30 日至 2 月 24 日第 1 次上網公告，2 月 24 日第 1 次開標，因投標廠商僅有 1 家，未達法定家數而流標，再於 109 年 2 月 25 日、3 月 24 日分別辦理第 2 次及第 3 次公開招標，經評選結果，因廠商平均總評分未達 70 分(不合格)，爰最有利標從缺並予以廢標。適逢新冠病毒疫情影響，整體期程須配合調整，爰調整系統建置期程，並納入未來可能所需之適當客服人力及簡訊通知經費，於 109 年 5 月 4 日至 5 月 28 日第 4 次公告招標，招標文件除明列 New eID 系統之原則需求外，為保持彈性，亦明列得標廠商須配合本部後續政策需要或實際需求調整相關專案工作內容，以完善 New eID 系統建置工作，5 月 28 日辦理開標，因投標廠商未達法定家數而流標，再於 109 年 5 月 29 日至 6 月 2 日第 5 次公告招標。

系統軟硬體的建置與管理，均遵循資安規範，依標準作業程序，自採購即開始過濾把關，並以管理面及技術面層層嚴密控管建置廠商，New eID 系統未來將建置於內政資料中心之內網環境中，兼具優質網路資安環境及完善整體資訊安全防護，符合資通安全管理法規範，執行資通安全責任等級 A 級之公務機關應辦事項，並導入資訊安全管理制度、資安監控中心等，且在行政院資安處與各機關單位皆已建立資安聯防機制下，持續提升資安防護技術，落實自我管理，降低各類資安風險。系統建置工作亦涉及與中央印製廠承作製卡之系統介接事宜，為確保系統設計、測試、整合測試及上線工作，符合需求及品質標準，本部於 109 年 2 月 14 日委由第三方獨立驗證與確認（IV&V）公司辦理系統面之監督、協調與驗證，目前已就中央印製廠承作製卡工作進行專案管控。

New eID 整體之資訊安全防護規劃，依行政院訂頒「資安產業發展行動計畫（107－114 年）」辦理，至少須提列總經費 5%計算，資訊安全總經費約為新臺幣 2 億 4 仟萬元，投入於印製作業之場地安全管理、晶片安全、資訊安全架構、VPN 網路及系統硬體、資訊安全教育訓練及系統安全進行稽核等資訊安全防護工作。又本部自 107 年起分階段汰換戶政事務所之端末工作站及老舊資安設備，提升戶政事務所資安防護能力，強化基層至中央之資安聯防體系，

爰除 New eID 換發所需經費外，亦提升地方資安設備，以共同保障資安與資訊服務不中斷。

為使各界安心，將對外公開程式源碼，但核心程式將交由第三方機構進行資安檢測。同時也會辦理賞金獵人競賽，開放民間測試，盡力完備資安作為後，再全面換證。未來，在 New eID 穩健推動後，才會進行行動身分證之研議推動，該行動身分證不是一張新的身分證，而係植基於 New eID 之上。

三、 法規面

依戶籍法第 59 條規定：「國民身分證全面換發期程及其他應遵行事項之辦法，由中央主管機關定之。」本部爰於 109 年 3 月 19 日訂定發布「國民身分證全面換發辦法」，考量自 108 年 1 月即擬具全面換發數位身分識別證計畫並擴大成立工作小組，進行全面換證之相關前置作業，爰該辦法溯及 108 年 1 月 1 日施行，以完備本次全面換證之程序；目前刻正依戶籍法第 52 條規定修正「國民身分證及戶口名簿製發相片影像檔建置管理辦法」（草案），該辦法增訂執行業務查驗卡面資料即可辨識身分時，不得強制讀取晶片資料、各資訊系統在儲存、傳輸或運用晶片資料時，應建立嚴密安全保護機制、晶片內之公開區、加密區資料，僅用於臨櫃身分識別及資料驗證，以及網路資料驗證，不可單獨作為網路之身分識別。上揭辦法均屬法律授權訂定之法規命令，非行政規則，其修訂均依行政程序法規定辦理預告，使民眾能事先瞭解並有參與及表達意見之機會，尚無行政機關任意修改、擴權之情形。

由於各國法制架構不同，經檢視愛沙尼亞身分證件法（計 43 條）與德國身分證及電子識別法（計 35 條）內容，多分別於我國戶籍法、電子簽章法、個人資料保護法及資通安全管理法、內政部憑證管理中心憑證實務作業基準（CPS）等已加以規定，並經該等法律主管機關檢視均無須配合修正。

再者，戶籍法係規範國民身分證之格式、內容、製發等事項，民眾領取身分證後要如何應用，涉及個人使用自由、相關社會活動及服務提供之需要，屬各服務之作用法規範範疇，爰無法於戶籍法規範身分證之使用場合。此外，各

公、私部門都會接觸到民眾個資，皆受個人資料保護法之規範，須善盡資料保護之責，如有違反該法規定，即應負民、刑事及相關行政責任，任何目的外之利用，均受到嚴格限制，不得任意擴大利用，New eID 將在該等法律基礎上進行製發及應用，無另訂專法之規劃。

目前國家發展委員會正就歐盟一般資料保護規範(GDPR)與歐盟諮商中，後續將依諮商結果，儘速提出個資法修正草案及個資保護獨立機關組織法草案。

四、 行政面

為使換證作業有一致遵循作業流程與標準，本部於 108 年 11 月 6 日擬訂「109 年全面換發國民身分證作業程序執行計畫」(草案)函請各直轄市、縣(市)政府表示意見，並於 108 年 12 月 18 日與各直轄市、縣（市）政府研討執行計畫內容，將配合「國民身分證及戶口名簿製發相片影像檔建置管理辦法」函頒實行。

為確保全面換證作業順利，本部另研擬小規模試行計畫，於換證初期選定部分縣市進行，由民眾自願申請 New eID 等事宜。

五、 宣導面

為宣導 New eID 功能與效益及全面換證之申請方式、領證方式、應備證件等作業程序資訊，已於 108 年 12 月 31 日函頒「109 年全面換發數位身分識別證宣導要點」，俾利各戶政機關辦理換證宣導事宜，同日亦提供海報及跑馬燈，函請各直轄市、縣（市）政府協助宣導。

本部於 109 年 3 月 19 日提供相關宣導海報，請警政、外交、衛福、財稅交通、文化等機關（單位）協助宣導，並於 109 年 4 月 13 日與太乙媒體事業有限公司簽約，持續辦理預告換發 New eID、New eID 功能、特色及安全性、小規模試行換證等宣導事宜。

小結

德國、愛沙尼亞早在十餘年前即推動全面換發 eID，雖曾發生資安事件，但未影響其推動 eID 政策，本部自 102 年起開始研議並廣納各方意見，於考量隱私保護、資訊安全、資訊自主、法源依據、使用原則及各界需要等意見，不斷調整規劃內容，有關現階段之規劃成果報告將放置於「New eID 資訊公開專區」，期盼各界不吝指教，提供各項完善數位身分識別證的具體建議，於系統建置及實施過程，公私協力一起把數位身分識別證做得更好、更周延！

第貳章、專案執行過程

壹、卡片(含晶片)及其製發管理相關議題研析

為規劃符合 New eID 產能之設備、數量及成本，規劃團隊訪談現行與製卡相關之廠商，蒐集卡片製發流程及安全管制作法，分析卡片與晶片結合所涉技術及此過程之防偽需求，以及他國發卡經驗等。

表 1：相關廠商訪談名單

序號	廠商
1	宏通
2	datacard
3	東元
4	台銘
5	新東亞
6	PCCW
7	Muhlbauer
8	VERIDOS
9	達洲
10	DNP
11	IDEMIMA
12	日本凸板
13	Gemalto
14	中央印製廠
15	Get group

貳、系統建置相關議題分析

為進行製卡整合作業與數位身分證應用，規劃開發 New eID 管理系統，作為 New eID 管理中心，整體系統設計與相關系統（自然人憑證管理中心資訊系統、戶役政資訊系統與製卡中心產線）整合，並包含 New eID 介接應用服務管理系統、API 應用程式庫開發、個人端及戶政事務所端維護軟體、機關端應用軟體、行動身分證軟體建置及 New eID 服務專區建置等。

為掌握現行自然人憑證管理中心運作現況及戶役政資訊系統運作現況，規劃團隊訪談現行維運廠商，以納入整體系統設計，並訪談我國其他憑證業者，以形塑本案系統建置之規劃建議。

表 2：系統建置規劃報告相關廠商訪談名單

序號	廠商
1	中華電信股份有限公司
2	資拓宏宇國際股份有限公司
3	臺灣網路認證股份有限公司

第參章、卡片（含晶片）規格及需求規劃

壹、New eID 設計式樣及印製內容

依據換發規劃案服務建議書所列之原則設計 New eID 卡面記載項目及欄位名稱如下：

一、卡片記載項目

（一）卡面規劃原則

1. 卡面個資最小化原則

New eID 基於個資揭露最小化、卡面公開個資降至最低，以及簡約設計等原則，將配偶、父母姓名等個人延伸隱私資料存放於晶片加密區內，另以簡約為基礎的設計元素，將卡片正面之記載欄位精簡設計，僅保留具有個人身分識別功能之欄位，如「姓名」、「統一編號」、「出生年月日」、「結婚狀態」及「相片」等。

2. 中英對照原則

New eID 卡面記載項目以中、英雙語，除可與國際接軌，更具實用性及前瞻性。

（二）卡面欄位

本次 New eID 卡面欄位名稱及內容規劃如下（卡片記載項目及方式彙整如表 3）：

1. 正面設計

(1) 記載當事人姓名資料包含中文姓名、外文姓名(目前規劃民眾自主選擇是否登載)，如有登記羅馬拼音者，應並列羅馬拼音，顯示欄位名稱「姓名」。

(2) 記載當事人統一編號，顯示欄位名稱「統一編號」。

(3) 記載當事人生日，顯示欄位名稱「出生日期」。

(4) 列印當事人相片，但不標註欄位名稱「相片」。

2. 背面設計

(1) 記載當事人結婚狀態為「有」、「無」，顯示欄位名稱「結婚狀態」。英文如記載「Yes」、「No」除不符英文習慣，「No」本身的否定意義更恐有歧視民眾之疑慮，建議逕以英文表單常見選項「Married」、「Single」之中性敘述。

(2) 記載製卡中心製證日期，顯示欄位名稱「製證日期」。

(3) 記載 New eID 應換發日期，顯示欄位名稱「應換領日期」。

(4) 列印卡片序號(即證件號碼)條碼，不標註欄位名稱「卡片序號」，但條碼下方顯示卡片序號，每張卡片出廠配號之卡號作為卡片序號。

(5) 列印國民身分證統一編號條碼，不標註欄位名稱「國民身分證統一編號」，且參考 94 年版之國民身分證，條碼下不顯示國民身分證統一編號。

(6) 列印依據 ICAO 9303 規定之機讀碼，不標註欄位名稱「機讀碼」，強化防偽驗證。

表 3：New eID 之欄位安排建議

中文欄位名稱	英文欄位名稱	位置	備註
姓名	Name	正面	
統一編號	ID NO.	正面	
出生日期	Date of Birth	正面	中文部分形式為「民國○○年○○月○○日」、英文部分

中文欄位名稱	英文欄位名稱	位置	備註
			使用西元紀年，形式為「yyyy/mm/dd」。（格式參考附註）
結婚狀態	Marital Status	背面	內容：中文為「有」、「無」，英文為「Married」、「Single」。
製證日期	Date of Issue	背面	日期形式同出生日期。
應換領日期	Date of Renewal	背面	日期形式同出生日期。
卡片序號(以條碼形式呈現)		背面	不標註欄位名稱「卡片序號」，但條碼下方應顯示卡片序號。
國民身分證統一編號(以條碼形式呈現)		背面	不標註欄位名稱「國民身分證統一編號」，且條碼下方不顯示國民身分證統一編號。
機讀碼	Machine Readable Zone	背面	欄位名稱「機讀碼」無庸顯示，直接顯示三排機讀碼。

附註：出生日期內的月份及日期，如為個位數字，即以一位數表示，如民國 95 年 8 月 5 日，西元 2006/8/5 月份及日期前面不補 0，中文及西元紀年採同樣作法標示。

二、New eID 式樣設計

建議規劃之 New eID 式樣係參考設計獎規劃之設計理念，並加入如玉山、玉山等高線等國家識別的重要表徵，並依 94 年版身分證，循例放置國旗。

另外卡面字型選擇上，基於中文姓名有罕用字考量，採目前戶役政資訊系統使用之國家發展委員會全字庫字體。另基於版面整體設計，其他字型採黑體，並應由系統建置商取得字型授權。

三、空卡規格

(一) 卡片材質

依照規劃原則，空白卡片採用 PC（Polycarbonate，聚碳酸酯）材質，彩色相片及雷射雕刻個資。

(二) 卡片耐用性、抗彎曲、耐磨、防水、抗污、耐高溫等規格

建議採用 ISO / IEC 10373 及 ISO/IEC 24789 國際相關卡片材質測試標準，以確保卡片耐久性可達 10 年使用壽命。

四、晶片規格標準

(一) ISO / IEC 相關標準：

1. ISO / IEC 7816：Information technology-Identification cards-Integrated circuit（s）card with contacts
2. ISO/IEC 14443： Identification cards

(二) ICAO Doc. 9303

(三) eletronic Machine Readable Travel Documents (eMRTD)

(四) 晶片通訊協定：

晶片規劃設計，需符合雙介面的資料存取方式，使用符合 PC/SC 規範之接觸式或非接觸式讀卡機，均需能正常讀取使用。晶片的存取介面說明如下：

1. 接觸式介面：需符合 ISO/IEC 7816 Part 3 T=1 的規範，工作頻率在 3.579 MHz 下，傳輸速率至少須能支援 115,200 b/s 以上。
2. 非接觸式介面：需符合 ISO/IEC 14443 Part 2-4，支援 Type A 或是 Type B 規範的 T=CL 傳輸協定，工作頻率在 13.56 MHz 下，傳輸速率可支援 106 kbit/s 、212 kbit/s 和 424 kbit/s。

(五) 晶片記憶體空間（EEPROM 或 Flash Memory）可實際儲存或使用的記憶體容量必須至少 120KB（含）以上。（目前晶片資料共約需 65-70KB 左右，晶片規格選擇係取決於目前市場主流，經蒐集資料顯示，目前晶片規格主要以 80KB 及 144KB 為主，如採用 80KB 扣除晶片作業系統(OS)所佔之空間，實際容量將不足 60KB，爰規劃建議採用 144KB 之規格。）

(六) 非接觸式介面感應距離只能在數釐米內。

(七) 晶片加解密安全功能需支援下列項目：

1. HRNG 硬體亂數生成器（hardware random number generator）或 TRNG 真亂數生成器（True Random Number Generator）。
2. DES 資料加密標準（Data Encryption Standard）。
3. 3DES （Triple DES）。
4. AES 進階加密標準（Advanced Encryption Standard），金鑰長度至少 256bits。
5. RSA 加密演算法（Rivest, Shamir and Adleman Encryption Algorithm），金鑰長度至少支援 2048bits（含）以上。
6. ECC 橢圓曲線密碼學（Elliptic Curve Cryptography），金鑰長度至少支援 384bits（含）以上。
7. 鑒於現行晶片多採用歐洲規格，且較為穩定，建議 SHA 安全雜湊演算法（Secure Hash Algorithm），需支援 SHA_224，SHA_256，SHA_384，SHA_512。
8. 卡片內產製金鑰對（on card key pair generation），私鑰（private key）不可匯出。

(八) 必須支援 ICAO BAC/SAC/EAC，PA 及 AA 資料讀取驗證標準。

(九) 硬體需通過安全認證 Common Criteria EAL 5+（含）以上，晶片須可防範電子 SPA/DPA（Power Analysis）、Trimming、DFA（Differential Fault Analysis）等攻擊，及可承受各式物理（電壓、音波、溫度、光）衝擊。(BSI-CC-PP-0084、BSI-CC-PP-0099、BSI-CC-PP-0084)

(十) New eID 使用之作業系統及應用程序（Applet）需通過安全認證 Common Criteria EAL 4+（含）以上。(BSI-CC-PP-0055、BSI-CC-PP-0056、BSI-CC-PP-0068、BSI-CC-PP-0059)

(十一) New eID 使用之作業系統及應用程序（Applet）須以 ROM 的形式燒錄於晶片中，且不得變更。

(十二) EEPROM 或 Flash Memory 的可讀寫次數壽命至少需 100,000 次以上。

(十三) 使用年限至少十年。

(十四) 採用雙晶片備援，確保晶片供應不致短缺，若遇晶片品質不符流通使用需求或有安全疑慮時，可及時啟動備援晶片。

五、晶片記載項目的作業規範

參照國際民航組織(ICAO)之電子防偽機制、存取控制機制，及其他相關之國際標準。

規劃晶片分為「戶籍地區」、「公開區」、「加密區」、「自然人憑證區」等 4 區。各區語言之使用原則，凡欄位內容如使用雙語記載者，欄位名稱亦應以雙語記載，民國、西元紀年並列。

內政部調整說明

原規劃分為「戶籍地區」、「公開區」、「加密區」、「自然人憑證區」、「ICAO 區」等 5 區。考量民眾恐誤解 New eID 亦可使用於國外通關，而未攜帶護照，為消弭疑慮，故關閉 ICAO 區，不寫入資料。

其中，公開區及加密區只用在臨櫃的身分識別及資料驗證，以及網路的資料驗證，不可作為網路的身分識別及簽章。如需簽章，則要當事人親簽文件才可；若 New eID 有附加自然人憑證可使用其自然人憑證於網路作身分識別及簽章。

New eID 係利用卡片之自然人憑證及密碼，作為本人使用網路身分識別之雙因子驗證依據，民眾應妥善保管卡片及密碼並慎選安全的電腦環境及可信賴的應用系統。各機關應依所提供服務之等級，輔以其他驗證配套機制。民眾及各機關的義務可參閱內政部憑證管理中心憑證實務作業基準。

主要區域規劃如下：

(一) 戶籍地區

1. 資料內容：戶籍地址（僅到村里鄰），僅有縣市、鄉鎮市區、村里、鄰、簽章值，無其他個人資料。
2. 資料讀取方式：可不輸入卡片讀取碼，方便即時讀取。
3. 資料顯示方式：以村里鄰代碼及中文表示，無法顯示罕用字之情況時，得用代碼搜尋，以解決罕用字無法顯示問題及創造便利性。

(二) 公開區

1. 資料內容：「姓名（中、外文）」、「統一編號」、「出生日期」、「戶籍地址」、「結婚狀態」、「役別」、「卡片序號」、「應換領日

期」、「製證日期」及「相片」共計 10 項及簽章值。前揭「戶籍地址」須記載完整戶籍地址。

內政部調整說明 為避免卡面的照片被偽變造，因此採電子防偽機制保護，將卡面列印之相片納入晶片公開區，透過晶片內存放之相片與卡面上之相片進行比對，強化防偽驗證。

2. 資料讀取方式：需符合 ICAO SAC（Supplemental Access Control）驗證，輸入讀取碼（CAN： Card Access Number，即卡片序號後 6 碼）或 MRZ 機讀碼才可讀取。

內政部調整說明 原規劃讀取碼為國民身分證統一編號後 6 碼。基於保障民眾隱私及提高安全強度，將讀取碼調整為卡片序號後 6 碼。

(三) 加密區

1. 資料內容：「配偶姓名」、「父姓名」、「母姓名」、「出生地」、「性別」及「讀取碼」（供調閱公開區資料使用）共計 6 項及簽章值。

2. 資料讀取方式：晶片內密碼驗證作法可參照歐盟公民卡規範 IAS-ECC 或 PKI 密碼驗證等同的機制；如民眾須輸入自訂密碼(6 位數字 PIN Code，下稱 PIN1)，且需用機關或服務提供機關(構)須向內政部申請讀取權限，作法需採用同 ICAO EAC（Extended Access Control）驗證方式後，始可讀取本區資料，且密碼連續 3 次輸入錯誤即鎖卡無法讀取。

內政部調整說明 原規劃加密區及自然人憑證區 PIN1、PIN2 皆為 6-12 位數字，考量民眾可能直接設定兩組相同密碼，致密碼防護機制不彰，爰調整規劃兩者長度不一致(PIN1，6 位數字、PIN2，

8-12 位數字），提高使用安全強度。

3. 本區域僅可使用接觸式讀卡設備，無法使用感應讀取。

內政部調整說明

原規劃本區域採雙介面讀取(插卡及感應)，為提升安全強度，故關閉本區域感應功能，改為僅能插卡讀取。

(四) 自然人憑證區

1. 使用方式：

民眾須輸入自訂密碼(8-12 位數字 PIN Code，下稱 PIN2)。驗證密碼成功後（密碼連續 3 次輸入錯誤即鎖卡），便可使用自然人憑證，作為簽章及加解密使用，本區需參照 PKI 規範，並僅可使用接觸式讀卡設備讀取。

內政部調整說明

原規劃加密區及自然人憑證區 PIN1、PIN2 皆為 6-12 位數字，考量民眾可能直接設定兩組相同密碼，致密碼防護機制不彰，爰調整規劃兩者長度不一致(PIN1，6 位數字、PIN2，8-12 位數字)，提高使用安全強度。

原規劃本區採雙介面讀取（插卡及感應），為提升安全強度，故關閉本區域感應功能，改為僅能插卡讀取。

2. 規劃內容：

(1) 規劃至少可產製 4 組非對稱式金鑰對（RSA 及 ECC）用於簽章及加解密等數位簽章應用，於卡片內產生非對稱式金鑰對。

(2) 規劃存放 6 組憑證，卡片發行時包含根憑證、中繼憑證、2 組金鑰對（RSA）及 2 組金鑰對（ECC）憑證，並可設定憑證存取權限，需輸入正確 PIN2 後，方可使用加密或驗證簽章。

(五) 安全驗證文件：

需提供 4 區安全機制的設計說明，說明如何防護及保護資料的安全性，並提出下列的安全驗證證明文件：

1. 晶片的硬體需提供 Common Criteria EAL 5+（含）以上的證明。

2. 作業系統（COS：Card Operation System）及 Java Card 平台需要提供 Common Criteria EAL 4+（含）以上的證明。

3. 本案採用之晶片內的各式應用程式（Applet）均需要提供 Common Criteria EAL 4+（含）以上的證明。

4. 提出強波器無法讀取晶片內容之證明。

5. 依本規劃提出 4 區安全設計參數並進行驗證。

(六) 晶片各區資訊變動以及資訊變動辦理方式整理如表 4。

表 4：卡片各區資訊變動辦理方式

晶片各區及其資料		不更換卡片情況下 變更資料之方式
戶籍地區	戶籍地址 （僅到村里鄰）	可異動，民眾需持卡至戶政機關更新。
公開區	中文姓名	不可異動。
	外文姓名	
	統一編號	
	出生日期	
	結婚狀態	
	卡片序號	
	應換領日期	
	製證日期	
	相片	

晶片各區及其資料		不更換卡片情況下 變更資料之方式
	役別	可異動，民眾需持卡至戶政機關進行更新。
	戶籍地址	可異動，民眾需持卡至戶政機關進行更新。
加密區	配偶姓名	可異動，民眾需持卡至戶政機關進行更新。
	父姓名	
	母姓名	
	出生地	
	性別	不可異動。
	讀取碼	
自然人憑證區	姓名	各欄位均不可異動。
	統一編號後 4 碼	
	憑證序號	
	憑證有效日期	

貳、卡片防偽變造設計

現行紙本國民身分證具有 21 項防偽變造設計，而 New eID 除物理防偽外，尚有晶片作業的資訊防偽，整體設計如下：

一、物理防偽

(一)規劃原則：卡面個人資訊採雷射雕刻文字。

(二)防偽變造設計（可視實際狀況選擇適用）

1. 扭索紋。

2. 彩虹隔色底紋。

3. 折光變色油墨。

4. 立體浮雕底紋。

5. 光影變化箔膜（OVD）。

6. 多重可變雷射影像（MLI/CIL）。

7. 浮凸觸感圖紋（tactile patterms）。

8. 浮凸雷射蝕刻文字（tactile laser engraving）

9. 影像透明視窗（Window）。

10. 顯性螢光設計（overt-fluorescent ink）。

11. 正面雙色隱性螢光圖紋（covert fluorescent ink）。

12. 背面隱性全彩螢光圖紋（covert fluorescent ink）。

13. 微細字（Micro text）。

14. 紅外線激發光油墨（IR Anti-Stoke）。

15. 以光學變化油墨、顯性螢光、隱性螢光、紅外線四者之一技術所設計之圖案或文字。

16. 以光學變化油墨、顯性螢光、隱性螢光、紅外線四者之一技術所設計之圖案或文字，且技術不與前款重複。

17. 廠商應至少提出 2 種須透過專屬設備查驗，否則無法查驗之防偽技術。

二、資訊防偽設計

（一）卡片序號：以流水號或其他具規則性之編碼所編製之號碼序列，為每張卡片所獨有。

（二）Chip ID：每張晶片獨有之 ID，僅作為生產履歷管理之用，寫入個人化資料時即封存。另須具備支援隨機產生序號的機制，在寫入個人化資料後啟動該機制，民眾使用時即產生不同的

隨機亂數，無從追蹤卡片，確保持卡人之個人隱私。

（三）公開區讀取碼：為卡片序號後 6 碼。

（四）加密區密碼 PIN1：與加密區相應之個人化密碼。

（五）憑證區密碼 PIN2：與憑證區相應之個人化密碼。

（六）晶片唯讀資料：晶片內僅「戶籍地址」、「役別」、「父姓名」、「母姓名」、「配偶姓名」、「出生地」、「戶籍地區」欄位資料得以更新，其餘資料以唯讀形式寫入，寫入後無法修改。

（七）機讀碼（Machine Readable Zone, MRZ）：本區域參照 ICAO 9303 文件規範，定義標準的資料格式，用以提供機器檢核個人資料。

（八）安全通道：除戶籍區外，所有訊息傳輸均應在安全通道的加密保護下進行，安全通道須採取足夠強度之演算法。

參、卡片（含晶片）安全防護措施

為符合晶片安全防護，建議採用以下機制：

一、 基本存取控制（Basic Access Control，BAC）。

二、 輔助存取控制（Supplemental Access Control，SAC）。

三、 被動驗證（Passive Authentication，PA）。

四、 主動驗證（Active Authentication，AA）。

五、 晶片驗證（Chip Authentication，CA）。

六、 終端驗證（Terminal Authentication，TA）。

七、 延伸存取控制（Extended Access Control，EAC）。

八、 密碼管理（PIN Management）。

九、 金鑰管理（Key Management）。

十、 安全通道（Secure Channel）。

十一、 存取條件（Access Condition）（如表 5）。

十二、 資料簽章。

表 5：卡片存取權限

卡片應用類別	最低存取權限
戶籍地區	無
公開區	安全通道+讀取碼或機讀碼 MRZ
加密區	安全通道+ PIN1 碼+ 檢核機關合法授權憑證（如 EAC）
憑證區簽章及加密金鑰使用	安全通道+ PIN2 碼

肆、相片規格建議

一、規劃作法

因 New eID 規劃參照 ICAO 規範，因此建議參照 ICAO 9303 之要求，現行《國民身分證及戶口名簿製發相片影像檔建置管理辦法》所規範之「國民身分證相片規格」宜配合修正，建議參考《護照條例施行細則》第 10 條所公告之《晶片護照相片規格》。

二、修正建議

鑑於現行紙本國民身分證與 ICAO 9303 之要求有若干出入，於部分較為嚴格、於部分較為寬鬆，本報告彙整如下表，並以接近或符合 ICAO 9303 之方向提出規劃：

表 6：New eID 相片規格修正建議

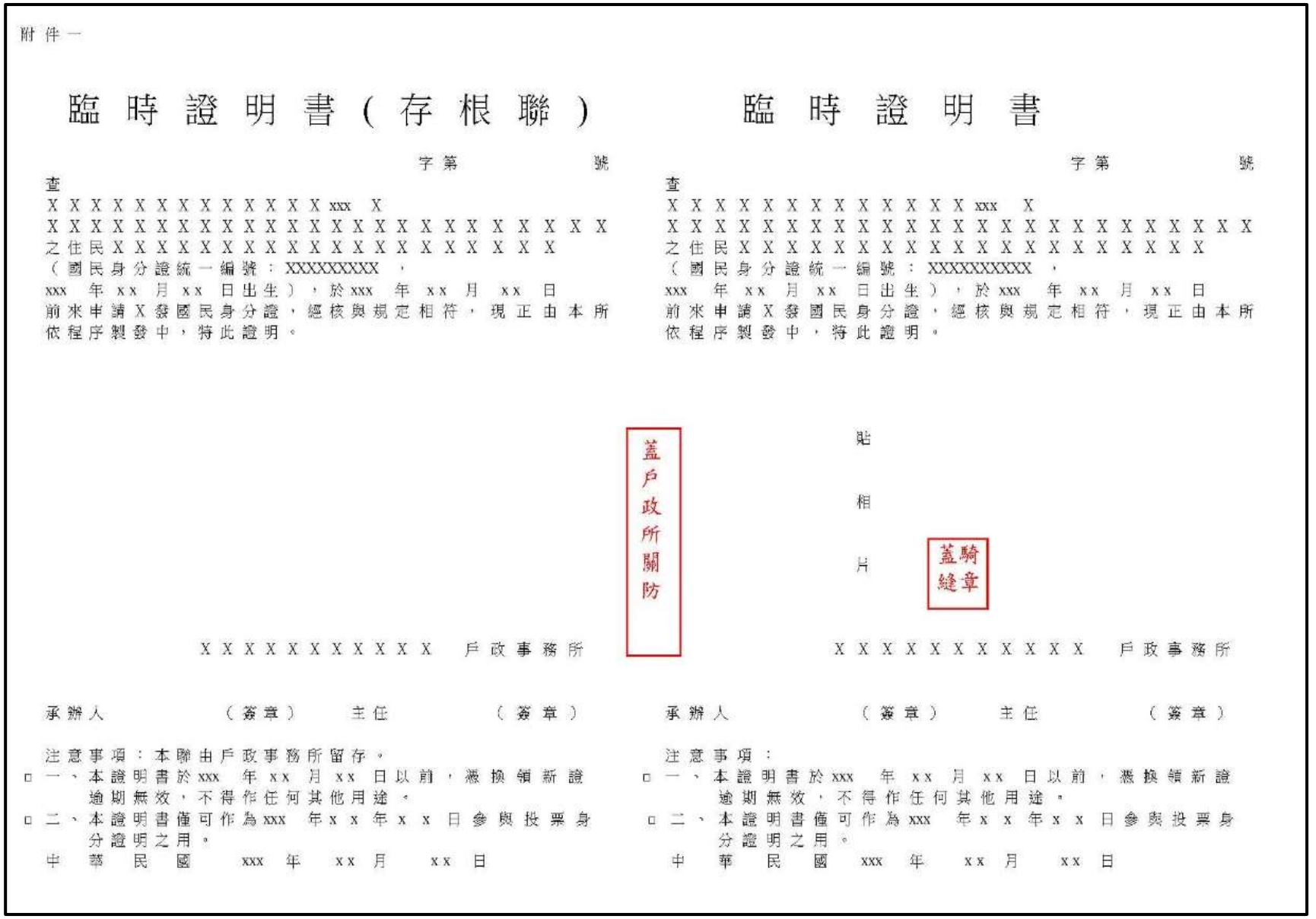
項目	現行紙本國民身分證	ICAO 9303、晶片護照	New eID 規劃
大小	直 4.5 公分，橫 3.5 公分，人像自頭頂至下顎之長度不得小於 3.2 及超過 3.6 公分。	直 4.5 公分且橫 3.5 公分（不含邊框），以頭部及肩膀頂端近拍，使人像自頭頂至下顎之長度介於 3.2 公分至 3.6 公分（亦即臉部佔據整張相片面積的 70～80%）。	無庸調整。
取像原則(含臨櫃作業)	尚無規定鏡頭至臉部距離	鏡頭距離臉部約 1.2 公尺（至少需 1 公尺以上）。	鏡頭距離臉部約 1.2 公尺（至少需 1 公尺以上）。
拍攝時間	最近二年。	最近六個月。	國內均以國民身分證作為辨識身分主要證件，且於確認人別時多係核對相片，就檢附之相片應有較嚴格規範，爰參考申辦護照規定，應繳交最近六個月拍攝相片。
修改與否	相片不修改，足資辨識人貌。	相片不修改且不得使用合成相片，足資辨識人貌。不得做數位影像的潤飾或補強。	規範仍應採取不修改、不合成，足資辨識人貌。不得做數位影像的潤飾或補強。
繳交數位相片	相片影像電子檔	（尚未開放上傳	電子檔規格限定

	規格限定JPEG格式,檔案大小不得大於 5MB，解析高度至少需達531像素，寬度至少需達413像素。	數位相片）。	JPEG格式，檔案大小不得大於5MB,解析高度至少需達 1,062 像素,寬度至少需達826像素。
相片不合規定之處理	倘所繳相片不符前述規定,應請申請人重新繳交相片。	倘所繳相片不符前述規定或經外交部領事事務局掃描器處理後影像品質未達標準，應請護照申請人重新繳交高列印品質的相片。 現行實務以電話通知護照申請人臨櫃繳交或郵寄至特定地址。	倘所繳相片不符前述規定，應請New eID 申請人重新繳交數位相片。

伍、製證期間 New eID 替代方案

根據現行《國民身分證及戶口名簿製發相片影像檔建置管理辦法》第18條第1項：「戶政事務所受理國民身分證請領申請，應於申請當日完成核發。但因製證機具故障、系統中斷、網路斷線或其他特殊情形，致無法於申請當日製發國民身分證時，得核發臨時證明書。」有關臨時證明書如圖1。

圖 1：舊版臨時證明書示意圖



附件一

臨時證明書（存根聯）

字第　　號

查
XXXXXXXXXXXXXXXxxx X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
之住民XXXXXXXXXXXXXXXXXXXXXX
（國民身分證統一編號：XXXXXXXXXX，
xxx 年xx 月xx 日出生），於xxx 年xx 月 xx 日
前來申請X發國民身分證，經核與規定相符，現正由本所
依程序製發中，特此證明。

蓋戶政所關防

XXXXXXXXXXX 戶政事務所

承辦人　　（簽章）　主任　　（簽章）

注意事項：本聯由戶政事務所留存。
□一、本證明書於xxx 年xx 月xx 日以前，憑換領新證
逾期無效，不得作任何其他用途。
□二、本證明書僅可作為xxx 年x x 年x x 日參與投票身
分證明之用。
中　華　民　國　xxx 年　xx 月　xx 日

臨時證明書

字第　　號

查
XXXXXXXXXXXXXXXxxx X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
之住民XXXXXXXXXXXXXXXXXXXXXX
（國民身分證統一編號：XXXXXXXXXX，
xxx 年xx 月xx 日出生），於xxx 年xx 月 xx 日
前來申請X發國民身分證，經核與規定相符，現正由本所
依程序製發中，特此證明。

貼相片

蓋騎縫章

XXXXXXXXXXX 戶政事務所

承辦人　　（簽章）　主任　　（簽章）

注意事項：
□一、本證明書於xxx 年xx 月xx 日以前，憑換領新證
逾期無效，不得作任何其他用途。
□二、本證明書僅可作為xxx 年x x 年x x 日參與投票身
分證明之用。
中　華　民　國　xxx 年　xx 月　xx 日

因 New eID 卡面顯示資料與現行國民身分證顯示資料有所不同，爰修正臨時證明書，其大小為 A4 或 A5 型式，樣式規劃如圖 2：

臨時證明書

姓名	蔾檥鼐		
出生日期	民國040年1月5日	性別	女
國民身分證統一編號	S232078441		
戶籍地址	新北市瑞芳區上天里001下天里２５４號		
申請時間	民國109年10月20日		
使用效期	民國110年1月19日		

注意事項：
(一)本證明書當事人申請國民身分證，經核與規定相符，現正依程序辦理中，特此證明。
(二)相關單位(人員)如須驗證其是否有效可至內政部戶政司全球資訊網（https://www.ris.gov.tw）查詢。
(三)憑本證明書於使用效期內親自臨櫃換領新證。
(四)本證明書使用效期，自核發日起3個月，但未屆3個月效期即領取新式國民身分證者，失其效力。
(五)本證明書請妥善保管，如於領證前遺失者，請於上揭戶政司網站或向戶政事務所辦理掛失作業，並向任一戶政事務所申請補發。
(六)臨時證明書於使用效期內與國民身分證的效力相同。

新北市瑞芳戶政事務所（職章）

列印日期/時間　109/10/20 02:19:14

臨時證明書檢查號：　20201020141016S232078441F120RY

圖 2：臨時證明書示意圖

考量民眾申請 New eID 至領取尚有一段製證期間，如有使用身分證明文件之需求，可向戶政事務所申請臨時身分證明書，內容包含姓名、出生日期、性別、國民身分證統一編號、國民身分證條碼、戶籍地址、申請時間、使用效期、相片及注意事項。其中，相片得由戶政事務所自系統內直接彩色列印，並新增國民身分證條碼以便臨時證明書得有較良好之應用；另提供 QR Code，以便民眾可隨時查詢國民身分證辦理狀態；另提供驗證序號，以便隨時查詢臨時證明書真偽。

臨時證明書設有使用效期，民眾於親自臨櫃換領新證時，宜繳回該臨時證明書，臨時證明書逾期或於民眾領取新證後失效，且不得作任何其他用途使用，將配合修正《國民身分證及戶口名簿製發相片影像檔建置管理辦法》第 18 條及附件一。

一、全面換發時期之配套措施

(一) 以現行紙本國民身分證申請換發 New eID 者

以現行紙本國民身分證申請換發 New eID 之民眾，申請時無須收回舊證，於領取 New eID 時，收繳現行紙本身分證，故該等民眾於全面換發時期尚無發給臨時證明書之需求。

(二) 現行紙本國民身分證遺失而逕申請補發 New eID 者

現行紙本身分證遺失之民眾，於全面換發期間須臨櫃申請補發 New eID，如有需求，可於申請補發 New eID 時併同申請臨時證明書。

民眾申請換發 New eID（無論是透過臨櫃或網路），於領取 New eID 前遺失現行紙本身分證者，因製卡至領卡尚有時間差，倘有身分證明之需求，可申請發給臨時證明書。

二、已完成 New eID 之換發者

民眾完成 New eID 之換發後，倘有遺失、申請戶籍登記導致卡面資料異動、卡片汙損而須申請換證時，倘有身分證明之需求，可同時申請臨時證明書，或得選擇使用行動臨時身分證（須視當時開發驗測行動身分證之期程而定）。

陸、卡片與憑證之效期運用

一、應換領日期說明

New eID 卡面記載之「應換領日期」，應與憑證之效期一致，憑證之效期須符合電子簽章法的 CPS 應載明事項規定，並遵照政府機關公開金鑰基礎建設憑證政策(GPKI CP)。

二、規劃作法

(一) 原則說明

規劃憑證之效期，以不超過卡片金鑰載具的生命週期為原則，是以卡片製造日期（即卡面記載之製證日期）為憑證之效期起點，並以卡面記載之應換領日期為憑證之效期終點。

假設 New eID 卡片金鑰載具的應換領日期設定為 10 年時，且憑證的效期為 5 年，憑證屆期時可再辦理 1 次憑證重新簽發，且憑證重新簽發作業僅適用於未被廢止之憑證。

民眾於 New eID 發放時選擇停用憑證時，憑證效期不因此而有所遞延。

(二) 卡片與憑證效期之運用情況

1. 憑證效期之計算

假設民眾取得製證日期為 110 年 7 月 1 日之卡片，應換領日期為 120 年 7 月 1 日者，則第一段憑證之效期應至 115 年 7 月 1 日，且不論其於何時更新第二段憑證，第二段憑證

之效期終點均僅能至 120 年 7 月 1 日，此規劃方式有利於憑證管理以及方便民眾記憶。

2. 不同年齡層之憑證效期（※以下規劃僅為草案，實際情形須以內政部憑證管理中心憑證實務作業基準內容為準）

(1) 未滿 65 歲之民眾

應換領日期配合憑證之效期，憑證屆期時可再進行憑證重新簽發作業 1 次。

(2) 65 歲以上民眾

New eID 不設應換領日期，其憑證重新簽發作業 1 次且到期後，若用戶仍有簽發憑證之需求時，則必須換發新 New eID 卡片。

第肆章、製卡中心規格、管理規範及安全規劃

為確保卡片製發場所及作業安全，爰就 New eID 製卡中心規格與地點評估、軟硬體及網路設備需求、建置與設備交付時程與數量評估、及其安全管制需求（如全天候保全錄影、無塵室人員進出管制，製卡設備、耗材、廢料處理、品管機制）、資安防護規範等面向提出規劃建議，建置廠商可視具體情況及實務需求進行強化調整。

壹、製卡中心規格與地點評估

製卡中心主要工作範圍為進行空白卡重置、卡片個人化作業及印製，最後完成封裝。為能在規劃的時程內安全順利地完成全國 New eID 的換發作業，因此製卡中心的規劃除了必須考量其產量外，也必須考慮其場所規格及地點，以利安全的生產並能快速送達戶所進行發放。

一、製卡中心規格

製卡中心作業區域依工作性質不同，區分為高敏感作業區及低敏感作業區。個人化區、初始化區及卡片儲存區域（按卡片生產狀況不同，區分為入庫區、倉儲區及出庫區）為高敏感作業區，其他區域為低敏感作業區。製卡中心空間規劃須符合內政部全面換發作業集中製卡產能所需，空間及規格須能達到每日最少產能 45,000 張卡片，實體空間安全設計也需要考量消防、空調、不斷電、門禁及監控系統等實體機房安全。

(一) 更衣區

作業人員自低敏感作業區進入高敏感作業區前需更換作業服裝，更衣區提供作業人員進出高敏感作業區更換作業服裝

所需空間，必需設備至少要有衣櫃存放作業服裝、鞋套櫃、頭套櫃等。

(二) 庫房

卡片動線為單向設計，全程監控管理，避免作業錯誤。相關建議如下：

1. 因製卡中心每日應最少生產45,000張，為確保庫存空間足夠，庫房應至少可存300萬張卡片之空間。
2. 庫房管理須區分管理品項類別，倘規劃為獨立作業者不得與該單位內的其他作業區共用,如空白晶片卡庫房、安全耗材庫房、壞卡及廢卡庫存區、出庫區存放製作完成之New eID。
3. 具備雙重安控（Dual Control）開啟大門，庫房須由鋼筋混凝土建造（最小15厘米或6英寸）或至少符合保險商研究室（Underwriters Laboratories）Class I盜竊認證標準。庫房外牆不能被作為主要壁面，且必須安裝強化後的不鏽鋼防盜門。

(三) 製卡作業區

製卡作業區空間規格評估需能達到預估產能（即每日45,000 張），並對所需之製卡相關設備數量及空間進行規劃，包含：每臺製卡機器產能估算、所需製卡機器數量估算、製卡機作業所需空間以及作業動線規劃等，且須保留操作人員作業空間與製發卡設備維修空間。

(四) 製發監控中心

1. 須通過 ISO 27001資訊安全管理認證。
2. 監控中心24小時都需有專業人員進行製卡中心安全監控，必須安裝CCTV，並進行人員進出管理，並留有紀錄。

3. 進出門須安裝自動關門裝置，門打開超過30秒，自動啟動聲響報警，門禁系統進出限單人進出，且只有授權人始可進出。

4. 監控設備須包含下列設備：

(1) 網路監控（網路狀況警示）顯示設備，負責監控製卡中心所有網路設備之實體連結狀況及顯示執行效率數據。

(2) 伺服器監控（系統效能之警示）顯示設備，負責監控製卡中心伺服器及應用程式之即時狀況數據顯示。

(3) 環境安全監控顯示設備，負責監控製卡中心相關區域之門禁狀況。

(4) 環境系統監控顯示設備，製卡中心專用的環境監控系統之機房空調、溫度、濕度、漏水、消防、門位、監視警報監測數據顯示。

(5) 電力系統監控顯示設備，UPS運轉狀況、電力供應來源及狀況、溫度及各項數值顯示。

(6) 消防系統監控顯示設備，極早期偵煙系統、光電偵煙及溫度系統數據顯示。

(7) 移動偵測器：於非作業時間進行移動偵測，偵測到異常移動則監控中心錄影主機產生警報聲，且警報信號將傳送到大門口警衛或警局。

5. 製發監控中心需建置相關整合性警告系統，提供以簡訊或電子郵件等通知功能，當上述各系統異常情況時，即時通知權責管理人員。

(五) 機房區

提供製卡中心運作時其系統主機所放置的空間，此空間須設置機櫃存放伺服主機及相關的網路與必須的機電設備。製卡中心標準系統主機機架規格及需求：

1. 機櫃寬度：至少標準19英吋（含）。

2. 機櫃尺寸：至少寬60cmx深100cmx高212cm。

3. 機櫃高度：至少42U。

4. 提供雙電源開關，面對面布置機櫃之間的距離不宜小於1.2m；背對背機櫃之間的距離不宜小於0.8m；機房搬運設備的通道淨寬不應小於1.5m。

5. 機櫃電力：

(1) 電力迴路具相互備援能力，機櫃供應電源採用雙迴路供應。

(2) 每條電力迴路提供單相110V、15A（含）電力。

(3) 具機房與不斷電系統提供備援電力。

(4) 特殊電力需求，如單相220V、三相220V等依需求建置。

(5) 每個機櫃提供電力容量限制至少在6KVA（含）以上。

(六) 消防設備

應具備全自動環保氣體滅火系統，並整合至環境監控系統，符合國內相關法規與標準。相關建議如下：

1. 消防設計須符合內政部消防署各類場所消防安全設備設置標準。

2. 將採環保氣體滅火設備，如FM-200環保藥劑氣體滅火器及自動排煙系統，作業區排煙窗加裝不銹鋼鐵網，保證證卡不會流出。

3. 警報系統採用偵煙及偵熱雙迴路系統，確保火警感知器正確性。

4. 消防系統設備採用標準火警分區安裝及火警分區動作。

5. 滅火設備動作時需有延遲時間（~30sec），以提供人員安全撤離防護區的需要。

(七) 空調

廠商需於製卡中心規劃智慧型輔助空調設備，將冷空氣傳送到需要加強散熱的機櫃，並偵測機櫃內的溫度，以調節風扇的轉速，達到節能的目的。相關建議如下：

1. 須有不同空調主機（水冷式或氣冷式，水冷式需搭配規劃水塔設備）作為備援並提供恆溫恆濕下吹式系統。中央電腦監控24小時專人監控，視當時環境溫濕度狀況進行遠端操作，以保持每區機櫃溫濕度的一致性。

2. 空調須達每坪一噸之標準，採用分區設置空調系統，以達到分區調節節能的目的。

3. 所有空調系統均接至緊急電源（發電機），且必須配置熱交換系統，將機房內熱氣與室外冷空氣對流。

4. 最佳溫度攝氏22ºC±2ºC、相對溼度50%±5%。

(八) 不斷電

為維持製卡中心的運作，須建置一套高效率不斷電系統設備，提供予製卡中心相關設備使用。機房電力相關建議如下：

1. 採雙路由機制供電，且互為備援，提高電力系統穩定安全。

2. 第二備援電力系統應可運轉24小時以上，UPS備載時間為滿載

30分鐘以上。

3. UPS採2N+1雙套備援建置，依據各樓層負載分別建置不同UPS。

4. 須有發電機與備援發電機，電力須有自動切換系統，雙管道間可於單一管道間發生問題時提供備援方案。

5. 機房需有至少3名專職機電人員並能提供專職機電值班人員7*24小時輪班。

6. 電源規劃參考美國電信產業協會（TIA）機房建置Rated3（含）以上TIA-942標準建置。

(九) 門禁

應有 RFID 感應或生物特徵安全功能機制，建置於製卡中心的機房及相關作業區，對相關人員進出進行安全管制，相關需求規格如下：

1. 廠區出入口設24小時專職保全人員，負責過濾人員進出及安全巡邏。

2. 製卡中心入口獨立門禁管制，並設專人管制製卡中心進出人員身分及設備，進出人員需經過RFID感應或生物特徵辨識方可進入門禁區域，如廠商或客戶有進入管制區域的需求，須提出申請經權責人員核准。

3. 於製卡中心出入口、初始化區、個人化區、倉儲區及機房區內部等區域，設置無死角CCTV監視點，24小時進行監控錄影，CCTV監控錄影以數位資料儲存、儲存期至少30天，可根據問題時間點進行調閱。

4. 機房區機櫃上鎖，機櫃門鎖統一控管。

(十) 環境監控系統

廠商需規劃1套製卡中心專用的環境監控系統安裝於機房區內，環境系統監控項目如機房空調、溫度、濕度、漏水、消防、門位、監視警報監測等，相關規格如下：

1. 空調系統監控：監測冷氣系統啟動、停止，可支援機房兩台空調系統自動交替運轉功能。

2. 環境溫度、濕度監測：須提供環境溫度、濕度監測。

3. 室內空氣品質：須符合環保署室內空氣品質管理法之相關要求。

4. 消防系統監控：含煙霧偵測、溫度偵測信號狀態及故障偵測。

5. 門禁監控系統：門戶啟閉狀態之監測、紀錄及傳輸。

6. 電力系統監控：各機櫃迴路電流監測紀錄及傳輸。

7. 提供以簡訊或電子郵件等方式，當上述各系統異常情況時，即時通知權責管理人員，且提供所有環境監測變數歷史資料查詢、列印及匯出功能，操作人員可根據查詢項目及日期時間，選擇列表、趨勢圖或統計長條圖顯示列印，匯出檔案須可轉存成CSV或TXT格式。

8. 所有通報系統之通報訊息會自動顯示於警訊通報視窗，並自動記錄於系統資料庫，以供操作人員隨時查詢。

二、製卡中心地點評估

製卡中心之地點，面積須容納前述製卡中心之規格外，製卡中心必須是具有高度安全保護環境的中央集中生產製作場所，製卡中心須符合 EMV（Europay, Mastercard, and Visa）、PCI-DSS

（Payment Card Industry Data Security Standard）或 ISO 14298 或其他相同等級之規範，及 ISO 27001 規範。

(一) 製卡中心外部

1. 外牆須採灌漿或石造或其他同等強度材質。
2. 門、窗戶或其他開口處必須以裝置施以保護，例如防竊玻璃、玻璃破碎偵測。
3. 靠近消防和警方單位，並應與警方單位連線，以能在合理的時間內進行援助，必須設置防闖警報系統進行保護。
4. 警報系統須配有備用電力或備用電池，以確保於電源中斷時可以繼續運作。
5. 所有出入點均須有 CCTV 監控。
6. 可利於通往屋頂之物品（例如樹木或柵欄）應拆除或搬遷，防止未經授權核可之進出入，且所有從屋頂進入之通道點應上鎖或從內部進行控管。
7. 建築物外觀不可有製卡中心或類似文字之標示。

(二) 製卡中心內部

1. 建築物主要進出口須設置訪客接待區，以限制訪客與接待人員實體接觸。
2. 製卡中心作業區域依工作性質不同，區分為高敏感作業區及低敏感作業區。個人化區、初始化區及卡片儲存區域（按卡片生產狀況不同，區分為入庫區、倉儲區及出庫區）為高敏感作業區，其他區域為低敏感作業區。

3. 高敏感作業區之進出必須通過門禁系統，一次一人進出控制，且嚴格限制授權人員才可以進出，並持續電腦連線監控和記錄所有員工及訪客之活動。最後一名人員離開時，門禁控制系統啟動警報系統，監控人員須可以收到警報訊號。

貳、軟硬體及網路設備需求

製卡中心所需之軟硬體設備必須能符合全面換發作業計畫所需。

製卡中心所需設備包含具有系統控制裝置（含軟體）、個人相片印製、雷射雕刻、晶片讀寫、QA 模組、封裝設備、進卡模組、清潔模組、出卡模組的製卡機、資料庫以及網路相關設備。有關個人化設備部分，卡片文字使用雷射雕刻方式，而卡片照片須為彩色，卡片須保證能使用 10 年。

因本案涉及國家安全，本案採購 PC 晶片卡（含晶片模組、作業系統及應用程序）及印製設備（含電腦設備軟硬體系統）之來源不可為中國大陸地區，並於交貨時提供原產地證明文件。

參、資料備份與災害應變

一、資料備份

(一) 程式與系統參數備份

1. 常態性備份：系統安裝完成後，完整備份。

2. 異動備份：透過內政部版控系統或手動記錄並備份歷次更新程式版本。

3. 快速安裝程序：透過可編輯安裝指令，建立系統環境自動安裝光碟，可於二小時內快速完成系統程式服務建置設定。

(二) 資料庫備份

建置廠商應規劃備份或備援機制，例如：週日全備份，工作日做異動備份。

二、災害應變機制

建置廠商應針對發生災害時，提出災害應變方案。

肆、安全管制需求規劃

New eID 為重要之身分證明文件，若發生保管不當致遺漏或盜取，將影響民眾權益甚鉅，製卡中心每日都應進行數量查核管控，核對入庫空白卡、半成品卡、成卡(送交戶政事務所)及製卡過程中卡片等數量進行檢查清點。

為達高強度的安全標準，製卡中心相關設計應參照國際標準 EMV、PCI-DSS 或 ISO14298 或其他相同等級之製卡安全規範，及 ISO 27001 資訊安全規範，並符合憑證實務作業基準規定之程序。

伍、管理規劃

一、作業內容規劃

表 7：作業內容規劃

組別	區域	作業內容
生產管制組	全區	生產流程管理、生產人員管理
生產作業組	初始化區	初始化、檢測卡片、產線控制
	個人化區	製卡、檢測卡片、產線控制
品管事務組	入庫區	入庫彙總、儲位編碼、庫房上架、揀貨、退貨
	倉儲區	入庫彙總、儲位編碼、庫房上架、揀貨
	出庫區	入庫彙總、儲位編碼、庫房上架、揀貨、出貨
	驗貨區	驗貨

資料處理組	製發監控中心	監控、工單派發、訂貨、稽核
安全管制組	機房/UPS	伺服器管理、網路設備管理、UPS 管理、稽核

二、管理規範

建置廠商應依照製卡中心實體環境針對下列4個面向(至少)訂定管理規範：

(一) 人為因素安全部分：須針對人為因素可能造成之安全問題進行管理，例如不安全動作、不安全環境、不安全設備等。

(二) 安全鑑別部分：如潛在危險因素、工作安全檢核點、工作安全分析等。

(三) 安全損失部分：如工作時間損失、原物料損失、設備損壞修復過程時間損失、生產時間損失等。

(四) 應變計畫：如失效應變計畫（作業面、系統面、卡片面）、資料外洩應變計畫。

陸、資安防護規範

一、製卡中心作業區電腦作業系統需至少佈署下列作業系統強化措施：

(一)具備安全開機（Secure Boot）機制，每次開機驗證作業系統未經竄改。建置廠商應提出此機制之詳細作法。

(二)禁止任何非作業處理用之程式執行。

(三)禁止連接非作業需求之IO裝置，如隨身碟等。

(四)禁止連接非作業需求之網路位址（IP）及埠口（port）。

二、由製卡中心 HSM 產製 DEK（Data Encrypt Key）於製卡機使用之發卡資料處理系統，製卡資料以 DEK 加密並以內網傳輸方式處理。

三、各子系統間資料傳遞媒介需主動加密保護，僅允許具有正確解碼程式及正確密鑰之讀取設備讀取及處理。

四、由製卡中心 HSM 產製初始金鑰（Initial Diversified Key）下載至晶片中，本金鑰用以確保晶片由初始化階段轉移至個人化階段（Personalization）過程中的安全，此程序應遵循 SCP03（Secure Channel Protocol 03）之規範。

五、HSM 產製金鑰之亂數產生器所產生的亂數應具有不可預測性及不重覆性。

六、所有製發卡相關作業皆須由專人負責（含發卡人員、卡片存放區作業人員、庫存管理人員、管制人員...等等），每人針對其職務給予不同之職務卡（含電子簽章）及授權碼，未經授權之人員不得進入相關系統，各項系統並須自動記錄相關人員所有之登錄/登出紀錄及執行工作內容。資料處理紀錄採用不可抹除或竄改之儲存方式唯讀保存。

七、每次系統啟動時須先執行電子簽章驗證作業，以確保發卡系統未經竄改，並偵測是否有外來軟體侵入。

八、發卡系統須經指定之安控人員身分識別後始可啟動。

九、HSM 須具備金鑰分持機制。

第伍章、製發管理規劃

壹、New eID 採購、製程、印製作業、資料及憑證寫入作業

本規劃係針對 New eID 採購、製程、印製作業、資料及憑證寫入作業等面向提出規劃建議，建置廠商可視具體情況及實務需求進行強化調整。

本案內容涉及國家安全，不允許大陸地區廠商、第三地區含陸資成分廠商及在臺陸資廠商參與。專案負責人及專案團隊成員不得為大陸地區人士；且廠商遵守本案之公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之廠商團隊成員，並應要求該等人員簽署與本條款內容相同之保密同意書、保密切結書及廠商人員接受適任性查核同意書，並應於決標次日起算 10 個日曆天內交付備查。

一、New eID 採購

（一）空白晶片卡採購

為確保空白晶片卡之安全性，承作卡片之生產廠於生產卡片時須取得 EMV（Europay, Mastercard, and Visa）或 PCI-DSS（Payment Card Industry Data Security Standard）或其他相同等級之規範認證，以確保空白卡產製及運送之安全性；且於執行空白晶片卡生產期間，採購方得隨時至卡片生產廠辦理查驗，廠商不得拒絕。

內政部補充說明

考量國際間有針對製卡核心之實體環境與製程安全進行規範之印刷產業安全印製標準尚有 ISO14298，且該標準設有印製政府部門等級安全文件之規範（Governmental level），與 EMV 及 PCI-DSS 除了產業別之差異外，其對場域與製程之安全要求相當，因此亦將該標準納入可取得之規範認證。

採購之空白晶片卡規格應符合「卡片（含晶片）規格及需求規劃」訂定之規格，並依規定製作卡體防偽措施，且晶片內容須已完成以下步驟：

1. 提供之應用程序至少需包含 eID 及 ePKI 等功能，即包含 PKI 及其他應用於本案 4 區（即「戶籍地區」、「公開區」、「加密區」、「自然人憑證區」）資料使用的相關應用程序。
2. 寫入晶片資料包含：Answer To Reset （ATR）與 Card Production Lifecycle Data （CPLC）；ATR History bytes 需根據買方需求做設定；CPLC 須包含晶片廠商資訊、晶片序號、生產批號等晶片相關資訊。
3. 設定卡片出廠金鑰，卡片金鑰須以約定之演算法計算並設定至卡片。
4. 完成空白晶片卡整批生產後，需產製卡片資料檔，其中卡片資料檔須包含晶片序號及 CPLC 等卡片資料，且卡片資料檔須以約定之演算法加密保護，並於交貨同時提供此資料檔。

（二）耗材採購

耗材可分為管制性耗材與非管制性耗材，廠商出貨耗材應檢附出貨單，出貨單內容須包含品名、規格、數量及批號，並提供 QR Code 條碼，條碼內需有上述之出貨單內容。管制性耗材為製發 New eID 晶片卡片之必要原料，如雷射蝕刻頭、彩色照片墨匣。非管制性耗材為輔助製發流程控管之原料，如信封、紙張、條碼碳帶、印表機墨水。

二、製程、印製作業、資料及憑證寫入作業

製發管理系統包含下列子系統：

(一) 製卡資料處理系統：包含卡片公鑰與 CSR 處理（傳送至 New eID 管理系統以利申請憑證）及卡片製發資料處理（卡片製發資料與卡片配對）。

(二) 個人化處理系統：

1. 初始化：為提高個人化作業正確性及縮短個人化作業時間之預先處理作業（例如確認晶片內程式正確性、金鑰預先產製 Gen key、CSR），預先寫入晶片內需要的 4 區資料空間。

2. 個人化：依據 New eID 管理系統提供的個人資料檔，寫入卡片需要的相關指令及個人化資料。

(三) 生產管理系統：卡片生產流程與狀態管控及耗材（製證耗材與空白卡）管理。

(四) QC 系統：檢查晶片出廠資料是否正確並與卡廠提供之資料比對，檢驗成功的卡片，將回饋檔拋轉製證管理系統及卡片管理系統。

貳、產品庫房管理

所有卡片及耗材管制作業系統流程中使用之相關表單除人工詳實填寫外，以生產管理系統作確實登錄，以方便稽查管理、管制、統計及相關報表之產生。另外，所有相關管制紀錄除交由製卡中心管控人員統整外，每日應上傳至相關稽核單位定時定期整理、分析，並必須存放至少十年，以備查驗。

一、庫房每日檢核

每日盤點作業，於系統停止作業時確認及清點空白卡、半成品卡、成卡、待出庫卡等及相關卡片耗材，並將製卡機台淨空。

二、庫房每月檢核

每月盤點作業於月底進行，於系統停止作業時確認及清點空白卡、半成品卡、成卡、待出庫卡等及相關卡片耗材，並將製卡機台淨空。

參、產品封裝檢測

New eID 製發完成在郵封前，須進行卡片品質檢測，以 QA 模組比對卡面印製資料之正確性，再通過人工品檢後之 New eID 以郵封機封裝。

肆、委託運送管理規範或準則

有鑑於 New eID 為重要身分證明文件，應使用安全委託管理方式運送，針對運送安全之需求依照運送階段不同，說明運送管理規範。

一、空白卡運送與包裝方式

空白卡運送包裝均需有獨立之溯源碼，外包裝需標註盒號、生產批號、產品名稱、作業系統名稱、PC 卡數量及製造日期等資訊並提供運送清單，並以 XML 格式儲存在 CD-ROM 光碟及其他儲存媒介中。

空白卡於陸上運送時全程須以保全車輛運送或押運，且需隨時有專職保全人員看管，並確保卡片包裝及數量之完整性。

二、成卡運送方式

每張卡片均裝在信封中，在信封上印有「申請案件編號」一維條碼及「姓名」，依戶所別封箱，封箱包裝均需有獨立運送編號（條碼）作為安全追蹤機制碼，並提供運送清單，建議每件封箱內卡片數量約 100 至 250 張，確保各戶所點收過程之正確性及便利性。

運送車輛不可有任何運送內容的標示或商標，卡片包裝需隨時有人看管，除非是在安全區域，如在運送期間臨停，承運人須確保卡片包裝之完整性。

有關運送頻率部分，建議採每星期運送 2 次，於收件當日或隔日送達戶所，避免影響領取進度。

伍、流程及安全控管機制

一、資訊安全規範

由於 New eID 涉及個人資料，為確保製證過程中個人資料受到保護，製卡中心應於 1 年內導入 ISO 27001 及 BS 10012 或 ISO 27701 或其他相同安全等級規範，並於 2 年內通過驗證，且持續維持其驗證之有效性。

二、安全控管

(一) 人員管理

1. 所有人員必須簽訂保密切結書。
2. 進行教育訓練。
3. 製卡中心所有作業均須專人負責，並依照職務給予不同之帳號權限控管，及記錄帳戶之所有工作內容及登出紀錄。
4. 人員異動或終止合約前，須解除或變更相關權限。
5. 因應資安政策，請勿攜帶手機及私人物品（相機、隨身碟、筆記型電腦、可拍照及具存取功能之 3C 用品等）入內。

(二) 進出人員管控

所有對外出入口（包括緊急出口）均應設有保全、警報及 CCTV，進出人員均須受到管控，並應依其職權設定被授權進入之區域，門禁系統記錄所有進出狀況，製證中心人員必須通

過主要進出口或員工專用通道進入,建築物外部進出口不可以直接進入管制區。

(三) 卡片控管

結合整體製卡流程及製卡設備,自空白卡入庫、製卡完成及運送後，皆應控管卡片之狀態。

陸、成卡品質需求及控管規範

首次製發前，印製樣卡經由相關人員審驗確認，制訂為符合品質之成卡樣本，並以儀器設備擷取相關數據，建立成卡品質標準。

New eID 製發後，QA 模組比對卡面印製資料之正確性，且卡片與設備須定期依照成卡品質需求及控管規範訂定之標準進行檢測。

發證人員並應以下列辨識步驟，控管成卡品質：（1）相片是否有污損。（2）證卡上文字是否清晰可見。（3）印製資料是否完整呈現。（4）依照防偽等級採對應之驗證方法。

設備廠商需提供定期檢測服務，以儀器確認 PC 卡材質與雷射雕刻與彩印效果，並調整機器參數，以符合成卡品質要求。

第陸章、API 應用程式規劃

New eID 管理中心整體系統設計，除須與現有系統介接整合外，並有 API 介接應用服務管理系統、API 介接應用程式庫規劃（包括個人端、需用機關、戶役政系統及憑證中心介接需求，線上系統及臨櫃介接需求等），整體系統架構如下圖所示：

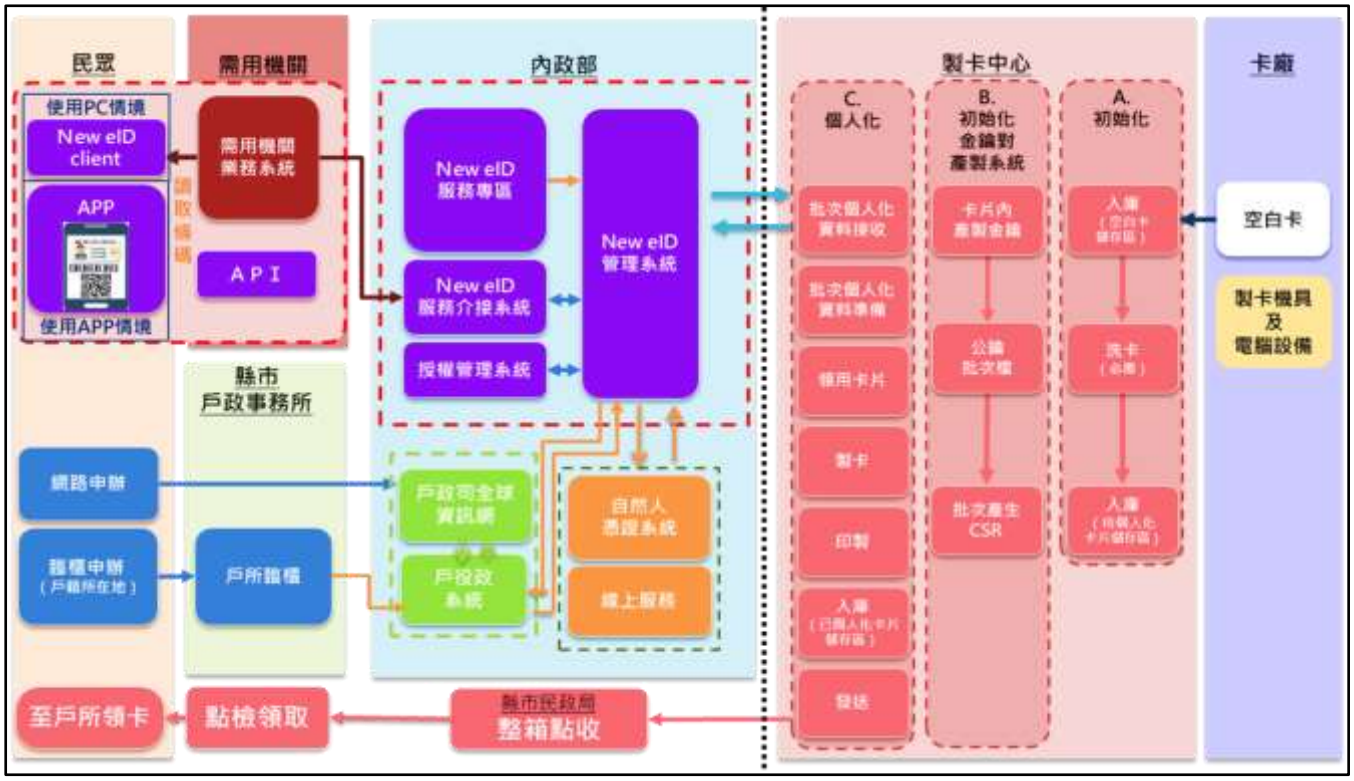


圖 3：系統架構與卡片製發管理整體架構圖

針對 API 應用程式、New eID 應用軟體及 New eID 晶片內容更新作法之規劃，內容包括：規劃 New eID 服務介接系統及功能、New eID API（N_eID-API）應用程式庫、New eID Client（N_eID-Client）規劃。

New eID 服務介接系統關係大致可分為內部服務型 API（包括：New eID 管理系統、製卡中心及內政資料中心）及外部服務型 API（應用端），各系統將由不同屬性的 API

做串接，如下圖：

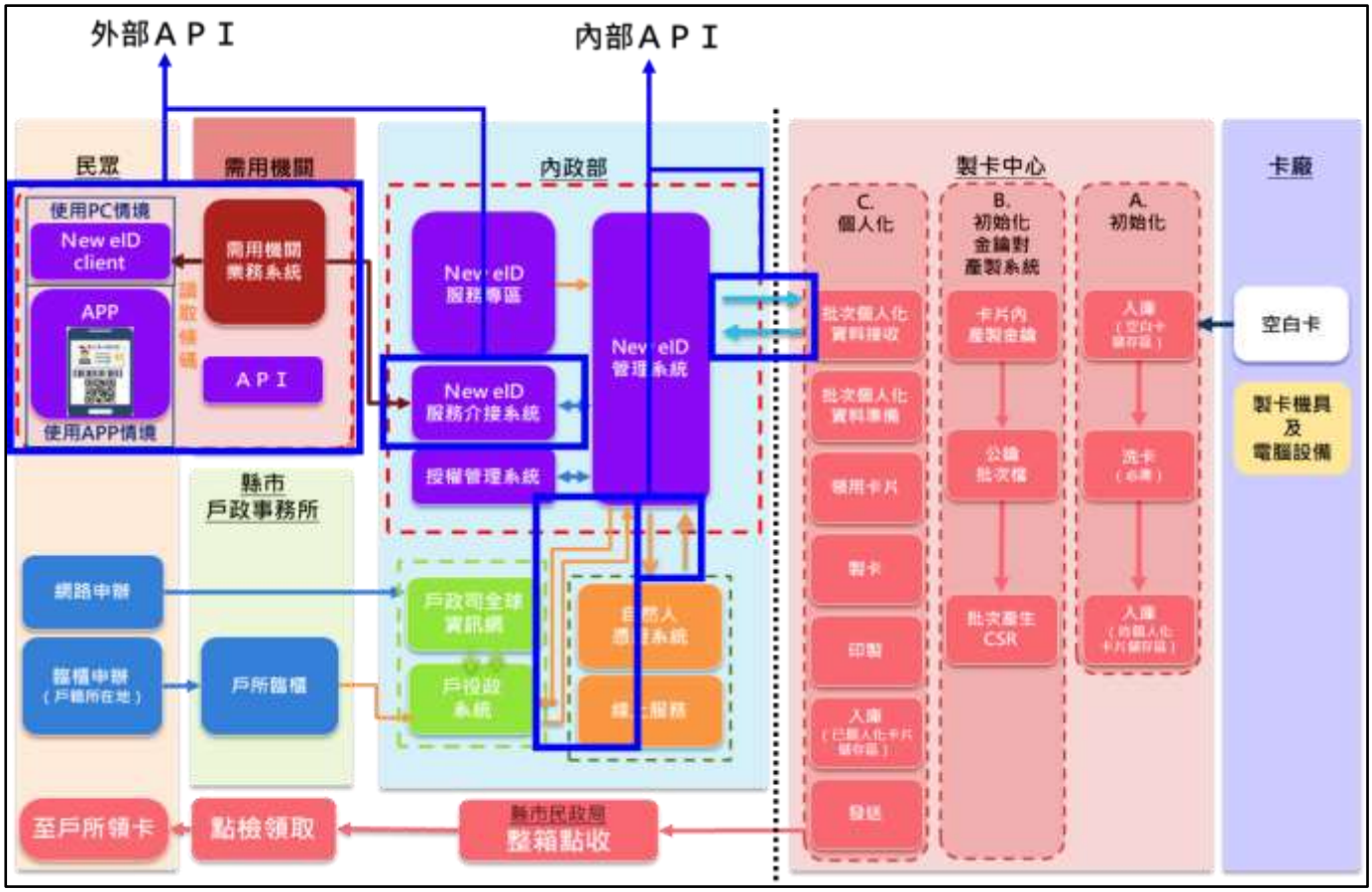


圖 4：New eID 服務介接系統關係圖

內部服務 API 串接可大致分為以下五類：

一、New eID 管理系統－製發管理系統。

二、New eID 管理系統－戶役政資訊系統。

三、New eID 管理系統－自然人憑證系統。

四、New eID 服務介接系統－自然人憑證系統。

五、New eID 服務介接系統－應用端。

外部服務型 API（應用端）依不同應用，可分為三類：

一、需用機關（構）業務系統（eService）與 N_eID-API。

二、個人查詢與管理 N_eID-Client。

三、行動身分證 APP（Secure API、Open API）（預計於第 2 階段推動）。

壹、New eID 相關應用情境說明

一、需用機關讀取晶片資料

(一) 公開區之 Open API

公開區採取 Open API 架構，需用機關可以直接下載 Open API，取得民眾同意後以接觸或非接觸方式經由讀取碼讀取公開區資料，如姓名、國民身分證統一編號、戶籍地址等。需用機關讀取公開區資料無須取得內政部授權且相關讀取紀錄不會連回內政部。

(二) 加密區之 Secure API

為保護民眾隱私，有關加密區資料採取 Secure API 架構，需用機關除須取得民眾同意且須輸入密碼（PIN1）外，尚須取得內政部之授權，始得以 Secure API 讀取加密區資料，以保護民眾相關隱私，例如父母姓名或配偶等資料。

需用機關每次使用 Secure API 時，內政部僅檢核其授權狀態。至於需用機關讀取民眾個人加密區資料之狀況僅記錄在其業務應用系統，不會記錄在內政部系統內，以維護民眾隱私活動。

(三) 加密區 Secure API 之管理機制

內政部對於加密區資料之隱私保護建立 Secure API 管理機制，並採取以下方式管理：

1. 以資通安全管理法之關鍵基礎設施提供者（如能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、政府機關、高科技園區）為優先申請對象，另非關鍵基礎設施提供者之政府機關亦可申請。

2. 對於加密區資料之調閱，中央目的事業主管機關得依據相關業務管理規範協調所管行業，依其需要申請Secure API。

二、民眾至戶政事務所進行晶片內容更新功能使用情境

（一）由戶政人員登入戶役政資訊系統依照資料更新作業流程進行更新。

（二）戶政人員再登入 New eID 管理系統進行晶片資料更新。

（三）在更新過程中，由 New eID 管理系統驗證晶片有效性後，New eID 管理系統向戶役政資訊系統查詢最新資料與晶片內之資料比對確認。

（四）New eID 管理系統，將會註記本次更新紀錄。

（五）最新資料再透過 New eID 管理系統私鑰(Document signer private key)進行雜湊簽章運算後傳遞至晶片完成更新。

三、個人端維護軟體功能情境與資安規劃

（一）進行晶片加密區資料檢視：

民眾於使用應用服務系統時，輸入卡片密碼（PIN1）後可檢視晶片內之加密區及公開區資料。

（二）因卡片密碼連續 3 次輸入錯誤，須進行鎖卡解碼

1. 民眾於 New eID 網頁專區輸入用戶代碼後，可進行鎖卡解碼。

2. 如忘記用戶代碼，則必須先於線上利用申請 New eID 時留存於 New eID 系統的 E-mail 或手機號碼進行 OTP 驗證後，於線上修改用戶代碼，或至戶政事務所修改用戶代碼後，再設定新的晶片密碼。

（三）變更卡片密碼（PIN1、PIN2）

民眾輸入原卡片密碼（PIN1、PIN2）驗證後，可變更原卡片密碼（PIN1、PIN2）。

（四）資安規劃

針對個人端維護軟體運作可能發生之資安風險，所採用之資安防護方法說明如表 8。

表 8：資安風險所採用之資安防護方法

流程	風險	資安防護措施
晶片至讀卡機	晶片偽造複製	• 唯一的非對稱式金鑰 • 內容無對外介面可以讀取，無法被複製 • CA （Chip Authentication）
	晶片被攻擊	• PIN 輸入及金鑰驗證失敗鎖定次數設定，防止蓄意暴力攻擊測試密碼 • 由 OS 層至應用層，金鑰驗證次數均有計數，防止惡意測試
	晶片資料竄改	• 在資料寫入時，針對各資料欄位做檢核運算，再將運算的結果以非對稱式金鑰加密簽章，確保資料的內容正確 • 部分資料為唯讀，無法被修改
	非授權讀取	• 使用 EAC（Extended Access Control）中的 TA（Terminal Authentication）用以檢核端末設備，是否授權可以讀取資料欄位，用以保護重要資料不被讀取 • 依據 ICAO 有 CA（Chip Authentication）機制用以檢核晶片內存的憑證是否合法，確認晶片的正確性
讀卡機至個人端維護軟體	資料側錄	• 端末資料傳遞建立安全通道（Secure Channel），內容均加密後傳輸
	側錄密碼	• 軟體安全鍵盤
個人端維護軟體至瀏覽器	資料側錄	• 端末資料傳遞建立安全通道（Secure Channel）
瀏覽器至新一代國民身分證管理服務	非授權讀取 資料側錄	• 使用 api_key、security_key 驗證 • 透過瀏覽器提供服務者應使用安全傳輸協定（TLS）進行資料傳輸

貳、New eID 身分證驗證管理架構安全規劃

一、功能架構

New eID 身分證驗證管理架構範圍包括：New eID 服務介接系統（N_eID-Server 加金鑰儲存），需用機關業務系統（eService），機關授權驗證管理系統（EAC-PKI）和民眾端讀卡程式（N_eID-Client）。

架構中所有模組都透過網路進行通訊，New eID 服務介接系統可以與需用機關業務系統（eService）、民眾端（N_eID-Client）及機關授權驗證管理系統（EAC-PKI）以加密協議進行安全通訊，如圖 5。其中 New eID 服務介接系統之說明如下：

（一）New eID 服務介接系統之作用

1. 使用New eID應用程式介面（API）與民眾端讀卡程式進行連結。
2. 與機關授權驗證管理系統（EAC-PKI）連結，進行資料驗證，確認其來自有效的晶片卡（New eID），並允許晶片卡確認需用機關業務系統的真實性。
3. 將身分證驗證的結果傳輸到需用機關業務系統。

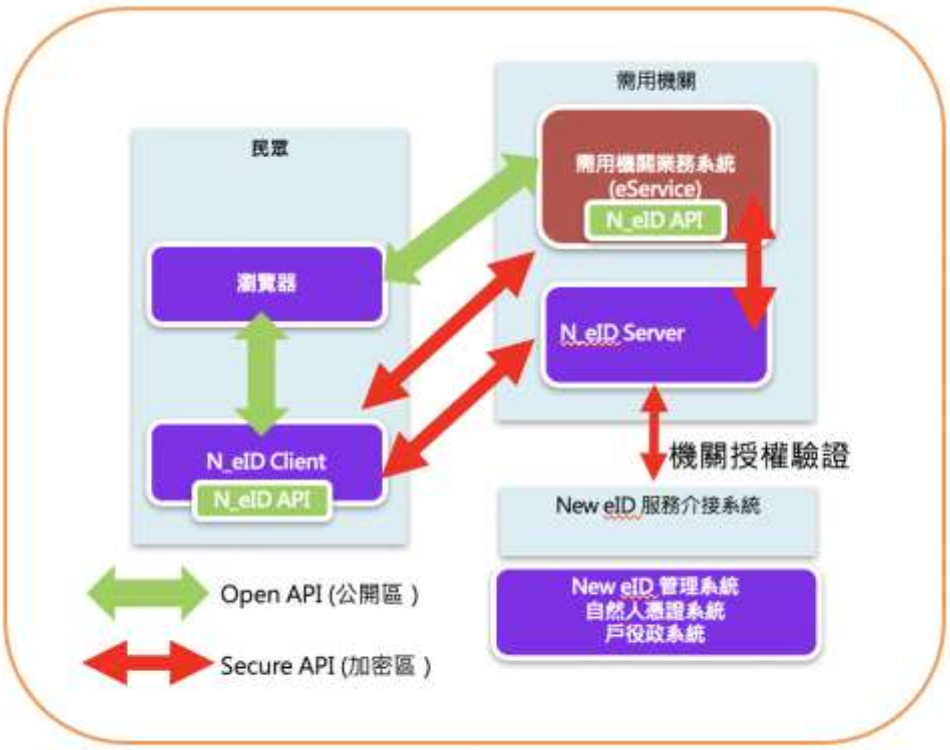


圖 5：標準需用機關系統（N_eID Server）規範架構

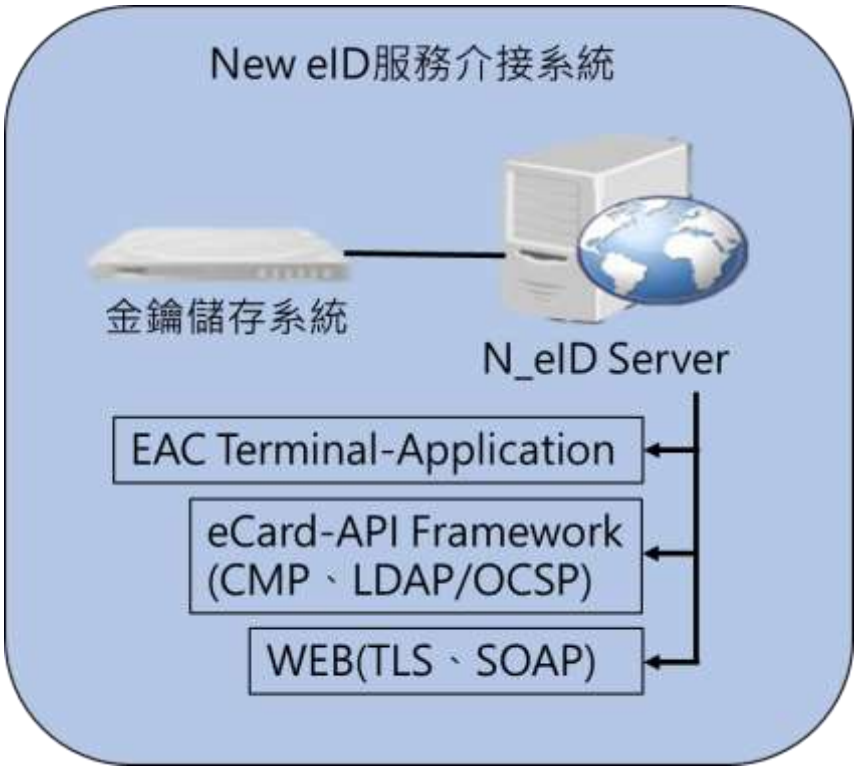


圖 6：New eID 服務介接系統

（二）New eID 服務介接系統功能要求

1. New eID 服務介接系統至少需要兩個資訊系統：
   New eID 服務介接伺服器（N_eID Server）和金鑰儲存系統（加密器）。

   (1) New eID服務介接伺服器：包含延伸存取控制（EAC）終端應用程式，New eID API和Web介面的資訊系統。

   (2) 金鑰儲存系統（加密器）：金鑰儲存系統是用於簽章建立和儲存終端授權憑證金鑰的核心模組，金鑰儲存系統直接連接到New eID服務介接系統。

2. 應用

   在 New eID 服務介接系統上運行所需的最小應用程式如下：

   (1) 延伸存取控制（EAC）應用：延伸存取控制（EAC）應用程式，使用New eID應用程式介面（API），從New eID讀取身分資料，並將這些資料提供給需用機關業務系統。

   (2) 網站服務（Web Services）：網站服務將New eID功能的協議及模組寫入，為需用機關業務系統提供對外入口。

   (3) New eID應用程式介面（API）框架：管理New eID服務介接系統和民眾端讀卡程式之間的通訊。

3. 通訊

   (1) 網路：透過網路存取，將New eID服務介接系統的

網站服務提供給需用機關業務系統或連接到民眾端，又出於管理目的，該網路(需用機關業務系統或民眾端)需要與New eID服務介接系統的網路進行連接。

(2) 協議：

A. New eID 服務介接系統、需用機關業務系統和民眾端讀卡程式之間的溝通，可使用 SAML、SOAP 或 RESTful 之協議，並使用安全傳輸協定（TLS）進行資料傳輸。

B. New eID 服務介接系統必須能夠存取機關授權驗證管理系統（EAC-PKI）的公鑰目錄（PKD）、憑證機構（CA）和憑證廢止清冊（CRL）。亦可使用輕量級目錄存取協議（LDAP）、線上憑證狀態協議（OCSP）和憑證管理協議（CMP）進行憑證狀態確認。應用系統可使用憑證廢止清冊或洋蔥路由器(TOR)以避免因使用線上憑證狀態協議(OCSP)導致用戶使用軌跡留於內政部。

二、安全準則

eID-Data 即儲存在 New eID 的民眾個人資料以及對民眾的 New eID 進行操作的結果，是受保護的資料。保護資料與資訊安全的機密性（不洩露資料）和完整性（驗證資料不被操縱、資訊的交換可被信任，即真實性）是最基本的要求，因此，New eID 服務介接系統的最終安全目標（SO）為：

SO1：必須保證 New eID 資料的機密性。

SO2：必須保證 eID-Data 的完整性（包括真實性）。

有關安全目標請參閱下表：

表 9：New eID 資料的基本安全目標

安全目標	說明
機密性 Confidentiality	eID-Data是保密的，未經適當授權，不得註冊、儲存或轉發。這特別適用於個人資料的讀取，包括eID晶片與資料接收者之間的通訊。**總體責任在於擁有授權憑證的實體**，該授權憑證用於讀取eID-Data。特別是，讀出的資料不得儲存在New eID服務介接系統（N_eID-Server）中超過特定驗證程式所需的時間。
真實性 Integrity	必須確保從eID以及與其關聯應用程式和系統（如New eID服務介接系統）中讀取資料的正確性。 eID-Data的真實性必須是可驗證的。同時，必須保證想要存取eID資料或至少參與該過程的人員和技術模組的真實性。

三、New eID 身分證驗證管理架構安全要求

(一) 組織資訊安全

1. 角色設定概念：採用以下原則制定及劃分角色權限。

(1) 職責分離。

(2) 定義各個角色與作業原則。

2. 角色權限分配原則（職責分離）：

(1) 系統負責人不得直接執行系統操作或系統管理工作，僅進行授權管理。

(2) 權限分配人員不得直接執行系統操作或系統管理工作，僅依授權情形進行權限分配。

(3) 具有管理權限者應有人數限制，其最基本的角色如下表。

表 10：角色說明

角色	說明
New eID服務介接系統的負責人	負責人對eID服務的組織單位負有完全管理責任。
New eID服務介接系統的IT安全官（ITSO）	IT安全官（ITSO）是管理團隊的一員，有助於與系統管理員一起完善系統安全原則，ITSO與系統管理員一起負責應用程式的管理，加密金鑰和憑證管理，網路和防火牆的管理以及設施存取控制。
系統管理員（S）	系統管理員（最好是一組）擁有eID服務的所有IT系統的最高權限，系統管理員負責實施備份，惡意軟體防護和定期更新保護措施。 管理員與ITSO一起負責管理應用程式、加密金鑰和憑證管理、網路和防火牆管理以及設施存取控制。
使用者	New eID服務的使用者，包括使用需用機關業務系統（eService）的民眾和需用機關，因為它們都使用New eID服務介接系統進行身分證驗證，使用者角色不可取得管理權限。

(二) 人力資源安全

員工在開始工作之前必須接受足夠的培訓，培訓必須至少包括對其任務的介紹和培養資訊安全意識。

負責人必須定期檢查員工的技術資格，以確定是否需要再培訓，如果角色設定概念（民眾除外）中定義的角色之一的人員無法履行其職責，則負責人應確保有合格的代理人。

(三) 存取控制

「存取」表示在使用資訊系統的功能時，系統上

即擁有民眾帳戶資料，因此，應建立紀錄和審查機制確保只有經過授權的人員才能使用。

1. 建立紀錄和審查存取機制。

2. 在存取概念中，必須根據角色概念定義，將具有保護要求的資料設定存取權限。

3. 必須根據角色概念及其排除的原則分配存取權限。

4. 必須確保儲存在金鑰儲存系統中資料（例如私鑰）的存取和使用原則。

5. 整個New eID服務介接系統的管理原則最低要求：

(1) 必須定義每個資訊系統都有足夠的存取機制來防止未經授權的存取。

(2) 必須定義資訊系統如何對單個角色進行身分識別，並應開發須滿足安全密碼使用規則的密碼指令。

(3) 遠端管理需要在存取概念中進行適當考慮，必須使用強驗證機制和強加密來保護通訊機制，且必須使用足夠的加密參數和演算法。

(4) 只有管理員才能進入New eID服務介接系統的所有資訊模組。

(5) 除網站服務外，民眾不得進入New eID服務介接系統的其他資訊模組。

(6) 必須根據角色概念及其排除的要求，分配New eID服務介接系統的許可授權。

(四) 加密

1. 使用加密控制的政策（加密演算法）

為了滿足 New eID 服務介接系統功能規範的加密要求，必須開發關於 New eID 服務的金鑰管理和憑證管理的加密演算法。此加密演算法必須考慮自然人憑證規範之金鑰長度和演算法，以及授權驗證系統要求。

管理員負責金鑰管理和憑證管理，以及請求憑證與私鑰的安全儲存。

(五) 實體安全管理

1. 設施門禁管理

開發與執行 New eID 服務介接系統之環境應具備門禁管理措施，進入管制區域的人數應限制在規定的最低限度。

2. 安全區域-物理安全邊界

(1) New eID 服務介接系統操作所需的資訊模組和技術設備必須託管在建築物內，建築物必須提供託管資訊模組和技術設備的安全區域。

(2) 備份資料必須儲存在代表單獨防火區域的安全區域中。

(3) 每個安全區域必須提供使用入口控制技術的入口控制服務。

(4) 必須至少建立一個危險警告系統，並確保警報立即發送給管理人員。

(5) 必須保護安全區域免受未經授權的進入，包括適當的存取控制系統和結構措施，建築基礎設施必須提

供高阻力，確保在警告管理人員到達之前保護未經授權的進入嘗試。

3. 安全區域-物理進入控制

必須檢查、監控和記錄安全區域的入口，並建立入口控制技術。

4. 安全區域-在安全區域工作

必須執行以下入口規則：

(1) 只允許管理員進入管理和託管資訊系統的安全區域。

(2) 所有其他角色和外部人員（例如訪客）之進出必須由管理員陪同。

(六) 營運安全

1. 操作程序和責任-變更管理

必須建立變更管理，包括硬體和軟體操作使用的生命週期法規，變更管理還包括新硬體和軟體的發布程式以及更新策略的規定。

在 New eID 服務介接系統的所有資訊系統上，應使用穩定且正式發布的硬體和軟體，必須根據條款 ISO27002 或類似操作軟體的控制來實施發布程式，推出程式需要明確定義的標準，包括新硬體和軟體的測試程式。

必須建立刪除硬體和卸載軟體的進一步標準，特別是資料媒體的處理很重要，必須確保殘餘資料被澈底刪除（例如破壞硬碟）。

2. 防範惡意軟體

除金鑰儲存系統之外的 New eID 服務介接系統都必須配備惡意軟體掃描程式，僅允許使用經檢查的無惡意軟體資料媒體。

3. 更新軟體

必須在 New eID 服務介接系統上安裝最新穩定版本，在更新軟體之前，必須考慮變更管理中定義的所有規則。

4. 記錄和監測

New eID 服務介接系統都必須具有日誌記錄功能，至少必須記錄以下事件：

(1) 系統登入（成功和失敗）

(2) 存取嘗試

(3) 存取權限異動

(4) 通過網站服務進行的存取

如果超過 3 次不成功的系統登入嘗試，則必須產生警報，管理員必須確認警報情況，讓資訊安全人員決定進一步的程序（例如關閉 New eID 服務介接系統或重置帳戶）。

5. 系統的安全安裝和安全操作

必須以安全的方式安裝和操作系統，且基於最小化、安全的操作系統來安裝和操作每個系統，並只使用 New eID 服務介接系統所需的功能，不得安裝 New

eID 服務介接系統不需要的軟體。

6. 系統的完整性保護

至少每週檢查一次 New eID 服務介接系統的每個系統完整性，並採取適當的措施，及記錄檢查結果。

如果完整性檢查失敗，則關閉受影響的 New eID 服務介接系統。

(七) 通訊安全

1. 網路安全管理 - 網路安全區域

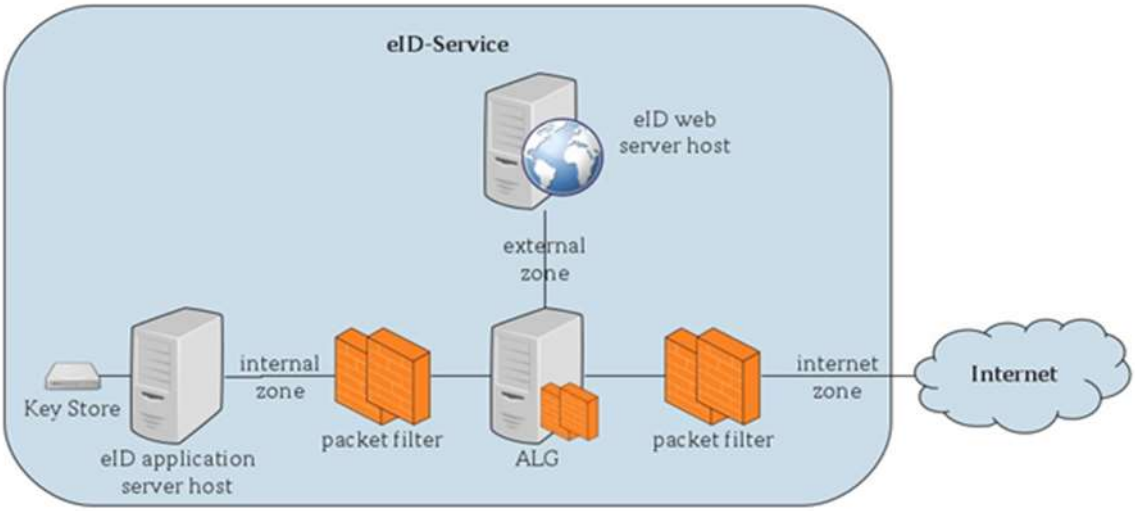
New eID 服務介接系統所在的本地網路必須分為三個安全區域：

(1) Internet區。

(2) 外部區域（DMZ）。

(3) 內部區域。

必須透過防火牆系統進行區域分離，New eID 服務介接系統必須分成兩個獨立的物理模組，即 eID Web 伺服器主機（Web 前端）和 eID 應用伺服器主機（應用伺服器），eID Web 伺服器主機必須放在外部區域中，eID 應用程式伺服器主機必須放在內部區域中，eID 服務透過 Internet 區域連接到 Internet。



2. 網路安全管理 - 防火牆系統（安全閘道）

如上圖所示，安全區域必須由防火牆系統（FW）分隔。防火牆系統必須是目前業界最新版本，應設計封包過濾器（PAP）、網頁應用級閘道（ALG）和另一個封包過濾器（PAP）的組合。

預設防火牆系統以防止透過 Internet 區域進行未經授權的存取嘗試。與外部實體的每次通訊都必須透過防火牆系統，此外，防火牆系統必須記錄所有連接。

應定期檢查日誌文件，至少每天檢查一次，並評估檢測到的攻擊和攻擊企圖，及進行適當的反應。如果記錄功能失敗，則必須向管理員發送警報，如果管理員無法重新啟動日誌記錄功能，則防火牆系統必須阻止所有通訊。

3. 網路安全管理 - 入侵檢測系統

為了檢測對 eID 服務的攻擊，必須建立最先進的入侵檢測系統（IDS），並在發生安全相關攻擊的情況下，向管理員發送可靠和迅速的警報。

IDS 必須支援以下分析模式：

(1) 基於簽章的檢測（通過與已知標準攻擊簽章進行比較檢測）。

(2) 基於協議的檢測（檢測協議違規行為）。

(3) 基於異常的檢測（檢測異常網路流量）。

(八) 供應商關係

若 New eID 系統交由委外服務系統商託管或開發，須向系統商提出需求說明，以滿足技術安全需求。

委外服務系統商應依照政府採購法相關規定，不得為大陸地區廠商、第三地區含陸資成分廠商及在臺陸資廠商。

(九) 合規-遵守法律要求

除了遵守所有適用的法律，所有安全措施亦須符合相關規定。

參、外部 API

New eID 之相關 API 需依據 eID 晶片內所採用之 Applet 功能及其所對應之 APDU 命令開發參考 ISO24727 之應用介面規範，及 New eID-Interface 規範 API、New eID 管理介面規範 API，自然人憑證相關 API 需依據 PKCS#11 之規範開發。

肆、內部 API 規格需求

一、自然人憑證系統介接需求

憑證註冊管理中心 RA 系統必須能連接 CA 系統、New eID 管理系統、卡管系統並提供以下憑證作業需求

功能項目：

(一) 提供 New eID 管理系統之戶所 RAO 系統可進行憑證管理作業及卡片管理作業之相關功能：

1. New eID 管理系統與 RA 系統驗證

2. 憑證簽發

3. 憑證停用/復用

4. 憑證展期

5. 修改聯絡人電子信箱/行動電話
（註：此資料會被用於民眾端解鎖卡功能，若使用行動電話發送簡訊會產生額外的費用）

6. 民眾憑證重寫

7. 查詢民眾憑證狀態

8. 修改憑證公布狀態

9. 民眾卡片臨櫃鎖卡解碼

(二) 提供一般民眾使用線上系統可進行憑證管理作業及卡片管理作業之相關功能：

1. 憑證停用/復用

2. 憑證展期

3. 憑證內容變更重發

4. 修改聯絡人電子信箱

5. 民眾憑證重寫

6. 查詢民眾憑證狀態

7. 修改憑證公布狀態

8. 民眾卡片鎖卡解碼

9. 民眾卡片修改 PIN 碼

(三) 提供 RA 系統與卡片管理中心作業之相關功能：

確認鎖卡解碼身分識別密碼。

二、戶役政系統介接需求

因應 New eID 換發，New eID 管理系統需介接戶役政系統，以進行個人資料查詢、換發證清單與個人資料傳送與狀態同步。

(一) 申請換證功能（依不同作業予以分檔）

1. 換發證申請成功名單與個人資料（此名單與檔案需依戶所區分檔案）。

2. 換發證申請失敗名單。

3. 瑕疵退回名單。

4. 例行換補證名單。

5. 卡面資料變更名單。

6. 撤銷請領證名單及掛失（撤掛）註銷名單。

(二) 整合換發證資料（包含個人資料、相片資料、憑證簽章等）並提供製卡檔進行卡片製發作業。

(三) 製發卡作業狀態回覆（完成後須刪除個人資料與相片）。

(四) 線上、臨櫃掛失（撤掛）註記。

(五) 卡片註銷註記（廢止、失效）。

(六) 進行相關卡片驗證程序以取出晶片內容。

(七) 臨櫃更新晶片內容。

三、製卡中心介接需求

因應 New eID 換發，New eID 管理系統需介接製卡中心，以進行製卡相關作業資料交換。

(一) 換發證名單與個人資料傳送。

(二) 預先產製之 PKI 金鑰（2 把 RSA 及 2 把 ECC）、空白卡晶片序號與 CSR 等卡片資料傳送。

(三) 製證之個人資料，相片檔案，自然人憑證等資料整合打包傳送。

(四) 瑕疵卡作廢重製作業

1. 瑕疵卡名單、瑕疵卡晶片序號、重製空白卡晶片序號與 CSR 等相關資料傳送。

2. 進行瑕疵卡狀態更新註記。

表 11：API 細部規劃功能清單

規範	功能	名稱
N_eID-Interface 規範	身分管理功能	GetCertificate
	簽章功能	SignRequest
		VerifyRequest
		ShowViewer
	加密功能	EncryptRequest
		DecryptRequest
eID 管理介面規範	N_eID_API 的管理	InitializeFramework
		TerminateFramework
		APIACLList
		APIACLModify
		FrameworkUpdate
		GetDefaultParameters
		SetDefaultParameters
	卡片管理	GetCardInfoList
		SetCardInfoList
		AddCardInfoFiles
		DeleteIDInfoFiles
	卡片終端管理	RegisterIFD
		UnregisterIFD

	可信檢視器管理	GetTrustedViewerList
		GetTrustedViewerConfiguration
		SetTrustedViewerConfiguration
		AddTrustedViewer
		DeleteTrustedViewer
	身分管理	GetTrustedIdentities
		AddTrustedCertificate
		AddCertificate
		ExportCertificate
		DeleteCertificate
		AddTSL
		ExportTSL
		DeleteTSL
	服務管理	GetOCSPServices
		SetOCSPServices（New eID Server）
		GetDirectoryServices（New eID Server）
		SetDirectoryServices（New eID Server）
		GetTSServices（New eID Server or MOICA）
		SetTSServices（New eID Server or MOICA）

ISO24727-3-Interface 規範（以 New eID Applet 功能為主）	卡片應用服務存取	初始化
		終止
		CardApplicationPath
	連線服務管理	CardApplicationConnect
		CardApplicationDisconnect
		CardApplicationStartSession
		CardApplicationEndSession
	卡片服務管理	CardApplicationList
		CardApplicationCreate
		CardApplicationDelete
		CardApplicationServiceList
		CardApplicationServiceCreate
		CardApplicationServiceLoad
		CardApplicationServiceDelete
		CardApplicationServiceDescribe
		ExecuteAction
	名稱物件資料管理	1. DataSetList
		2. DataSetCreate
		3. DataSetSelect
		4. DataSetDeletc
		5. DSIList
		6. DSICreate
		7. DSIDelete

		8. DSIWrite
		9. DSIRead
	加密服務	1. Encipher
		2. Decipher
		3. GetRandom
		4. Hash
		5. Sign
		6. VerifySignature
		7.VerifyCertificate
	差異身分服務	1. DIDList
		2. DIDCreate
		3. DIDGet
		4. DIDUpdate
		6. DIDAuthenticate
		5. DIDDelete
	授權服務	1. ACLList
		2. ACLModify
	IFD 接口規範	EstablishContext
		ReleaseContext
		ListIFDs
		GetIFDCapabilities
		GetStatus
		等候

		取消
		ControlIFD
	卡片功能	1. 連接
		2. 取消連接
		3. 開始交易
		4. 結束交易
		5. 發送
	用戶交互功能	1. 驗證用戶
		2. 修改驗證資料
		3. 輸出
讀卡機事件-Callback-Interface	IFD-Callback-Interface 可從終端層上方的層中獲得，並且包含 SignalEvent 功能	SignalEvent
自然人憑證 API 說明	初始 PKCS11 模組函式	InitLibrary
	結束 PKCS11 模組函式	CloseLibrary
	讀取 PKCS11 模組描述函式	HiSecureFunction
	讀取 Slot ID 函式	GetSlotID
	讀取 Slot 描述函式	GetSlotDesc
	測試 Token 就緒函式	IsTokenPresent

	讀取 Token 描述函式	GetTokenLabel
	讀取 Token 序號函式	GetTokenSerialNumber
	登入 Token 函式	LoginToken
	登出 Token 函式	LogoutToken
	讀取金鑰數目函式	GetKeyNum
	讀取指定金鑰 ID 函式	GetKeyID
	讀取指定金鑰控制代碼函式	GetKey
	釋放指定金鑰控制代碼函式	FreeKey
	取得金鑰類別函式	GetKeyType
非對稱式加解密函式	基本簽章函式	BasicSign
	基本驗章函式	BasicVerify
	基本加密函式	BasicAsymEncrypt
	基本解密函式	BasicAsymDecrypt
	ECDH 金鑰生成函式	GenSessionKeyECDH
	ECDH 金鑰導出函式	DeriveSessionKeyECDH
憑證解析	讀取憑證數目函式	GetCertNum
	讀取指定憑證 ID 函式	GetCertID

	讀取指定憑證函式	GetCert
	解析憑證資料函式	DER2Cert
	編碼憑證資料函式	Cert2DER
	釋放指定憑證函式	FreeCert
	取得憑證之公開金鑰函式	GetCertPublicKey
	檢驗憑證簽章函式	VerifyCert
	取得憑證序號函式	GetCertSerialNumber
	取得憑證主體 DN 函式	GetSubjectDN
	取得憑證發行者 DN 函式	GetIssuerDN
	取得憑證效期開始日期函式	GetNotBefore
	取得憑證效期結束日期函式	GetNotAfter
	取得憑證主體別名（Email）函式	GetSubjectAltName
	確認憑證金鑰用途函式	IsKeyUsageEncipherment
	確認憑證金鑰用途函式	IsKeyUsageKeyAgreement
	取得憑證的 CRLDistributionPoints 函式	GetCRLDistributionPoint
	取得憑證的 SubjectDirectoryAttri	GetSubjectTypeOID

	butes 子項目之一subjectType（主體型別）函式	
	取得憑證的SubjectDirectoryAttributes 子項目之一HolderRank（正附卡別）函式	GetSubjectHolderRank
	取得憑證的SubjectDirectoryAttributes 子項目之一TailOfCitizenID（國民身分證字號後四碼）函式 b	GetTailOfCitizenID
	取得憑證的SubjectDirectoryAttributes 子項目之一，實體（機關、單位等）OID 函式	GetEntityOID
	取得憑證的SubjectDirectoryAttributes 子項目之一，統一編號函式	GetUniformOrganizationID
	取得憑證的SubjectDirectoryAttributes 子項目之一，群組代號函式	GetCertTypeID
	取得憑證的SubjectDirectoryAttri	GetCertTypeID

	butes 子項目之一，憑證類別代號函式	
	取得憑證的 SubjectDirectoryAttributes 子項目之一，UID	GetUID
	取得憑證的 SubjectDirectoryAttributes 子項目之一，卡號函式	GetCardID
	取得憑證 CAIssuers 函式	GetCAIssuers
	取得憑證 OCSP 位址函式	GetOCSP
	取得憑證的 AuthorityKeyIdentifier 函式	GetCertAuthorityKeyIdentifier
	取得憑證的 SubjectKeyIdentifier 函式	GetSubjectKeyIdentifier
	取得憑證的 CertificatePolicy 函式	GetCertPolicyOID
	取得 DER 衍生格式 GetExtensionDER	GetExtensionDER
	取得金鑰使用範圍	GetKeyUsage
	取得憑證 AuthorityInfoAccess 函式	GetAuthorityInfoAccess

	GetSubjectDirectory Attribute	GetSubjectDirectoryAttribute
	由 PKCS#7 憑證串列取得憑證函式	P7B2Cert
	取得憑證簽章演算法函式取得憑證簽章演算法的 OID	GetCertSignatureAlgorithm
	取得簽章憑證函式	GetSignatureCert
	取得加解密憑證函式	GetEnciphermentCert
	取得簽章金鑰函式	GetSignatureKey
	取得加解密金鑰函式	GetEnciphermentKey
CRL 解析	解析憑證廢止清冊函式（CRL）	DER2CRL
	釋放指定憑證廢止清冊函式（CRL）	FreeCRL
	驗證憑證廢止清冊函式（CRL）簽章函式	VerifyCRLsignature
	取得憑證廢止清冊函式（CRL）發行者 DN 函式	GetCRLIsseurDN
	取得憑證廢止清冊函式（CRL）此次更新日期函式	GetThisUpdate

	取得憑證廢止清冊函式（CRL）下次更新日期函式	GetNextUpdate
	取得憑證廢止清冊函式（CRL）的AuthorityKeyIdentifier 函式	GetCRLAuthorityKeyIdentifier
	取得憑證廢止清冊函式（CRL）的序號函式	GetCRLNumber
	取得最新憑證廢止清冊函式（CRL）位址函式	GetFreshestCRL
	取得最新憑證廢止清冊函式（CRL）位址函式	GetDeltaCRLIndicator
	檢查憑證是否含於憑證廢止清冊函式（CRL）函式	CRLSearchCert
	檢查憑證序號（SN）是否有含於憑證廢止清冊函式（CRL）中函式	CRLSearchSN
	取得憑證廢止清冊函式（CRL）的某一筆資料函式	GetCRLRevokedCert
	取得 CRL 簽章演算法函式	GetCRLSignatureAlgorithm

OCSP 操作	線上憑證狀態查詢函式（OCSP）	OCSPCheckSN
	線上憑證狀態查詢函式（OCSP）	OCSPCheckCert
通訊連結安全	一般安全要求	
	ISO/IEC 24727 協議	
	GetCertiftcate 的協議	
	遠端更新協議	

伍、 結論

本案參考歐盟近年來各國標準，其中包含德國與愛沙尼亞的 eID 整體架構規劃。

各項安全讀取模式，如加密區之 Secure API 即用於讀取晶片時之身分識別與管制，並搭配整體 N_eID Server 安全管理，如角色分層管理、存取控制管理等，以達到保護資料之目的，又個資需用機關讀取 New eID 須依個資法負個資保護責任，內政部只檢核個資需用機關之 Secure API 之授權狀態，不記錄個資作業細節，以釐清個資保護責任歸屬。

第柒章、自然人憑證規劃

規劃數位身分識別證（以下簡稱 New eID）附加自然人憑證，並可由民眾依其意願選擇是否申請及使用憑證功能。

內政部調整說明

考量各界仍有卡式自然人憑證使用需求及尊重資訊自主權，未來自然人憑證管理中心將持續營運，現行自然人憑證亦將續發。個人於填寫 New eID 申請表時可勾選不申請自然人憑證，將不會產製個人之自然人憑證並關閉晶片之自然人憑證區域(不寫入任何資料)；已申請者，亦可隨時決定停(復)用或廢止 New eID 晶片內自然人憑證功能。

壹、新舊憑證整合機制

New eID 晶片內所存放之憑證發行，採新建發證系統抑或整合現行自然人憑證發證系統將有所不同，爰關於新舊憑證之議題，規劃如下：

一、憑證發證系統規劃

由於 New eID 採用之新晶片已能克服舊自然人憑證未能開放 API 之爭議，且考量對現有應用機關之衝擊及憑證建置，如成立新憑證管理中心需經金鑰產製儀式、GPKI 憑證推行小組核可及經濟部審驗憑證實務作業基準等行政程序，其整體建置新憑證管理中心時程與成本都較沿用現行憑證管理中心高，故採取整合現行自然人憑證發證系統。

二、新舊自然人憑證規劃

因應 New eID 憑證載體變更，應用機關之應用系統介接新卡片需要至少 1 年以上準備時間，而憑證管理中心對應用 API 之設計應以最大方便性及匹配性為原則。於設計時，確認是否新 API 介面可沿用舊的 API 介面，若可，則應用系統程式僅需重新建立即可，新 API 自行判斷用戶卡片之新舊，再執行各流程。若否，則建立新 API 時，應本流程相同之原則，由應用系統程式修改呼叫 API 介面。因流程相同，按照修改指引置換 API 程式即可。

目前自然人憑證應用，有提供專屬外國人的自然人憑證，稱作「外來人口自然人憑證」，其可使用自然人憑證為個人綜所稅結算申報、勞工保險局 e 化服務系統、全民健康保險個人健保資料網路服務作業、線上申辦入出國日期證明書等，若取消非我國人之自然人憑證申辦，則目前我國政府機關公開金鑰基礎建設 GPKI 下並無其他適宜的憑證管理中心可提供替代，將造成非我國人者，無憑證可供其使用之困境。

在擴充現行自然人憑證管理中心之規劃下，採取一人多憑證之開放政策，憑證本質係資料加解密及數位簽章，民眾可依不同用途選擇使用不同張之憑證 IC 卡片。例如，現有自然人憑證作為公務識別證仍可繼續使用或外國人仍可申請自然人憑證。本規劃採取現行自然人憑證擴充，即現行之自然人憑證晶片卡維持發行，以兼顧外國人或滿足民眾使用憑證需求，讓自然人憑證使用上更加多元化。

另應於服務專區網站，提供用戶網站解鎖卡、修改 PIN2 碼、停(復)用等需求。

貳、憑證管理中心及卡管中心規範與備援機制規劃

一、憑證管理中心職責及義務

(一) 憑證管理中心之職責

1. 訂定、公告與管理憑證業務範圍內的憑證實務作業基準與憑證運作的相關作業規範。

2. 確認用戶憑證管理中心與註冊中心的權責關係，且註冊中心的實務作業必須依本作業基準與憑證政策及相關的規範運作。

3. 確認憑證系統作業人員（含合約委外人員）的選用與系統運作符合憑證實務作業基準的規範。

4. 作業人員必須善盡保管用戶註冊與憑證資料及相關訊息之責任，避免相關資訊洩漏、被冒用、篡改及任意使用。

5. 依照憑證實務作業基準的規範，接受用戶（註冊中心）憑證的申請、更新、停用、廢止、查詢及有關註冊申請訊息，確認註冊中心及用戶發送至用戶憑證管理中心之相關交易訊息的正確性與完整性，並執行憑證簽發作業及將相關回覆訊息正確且安全的遞送至用戶。

6. 依據憑證作業規範將用戶與本憑證管理中心的憑證及廢止憑證清冊正確且安全的遞送至儲存庫。

7. 必須與用戶詳細說明憑證申請、更新、停用、廢止、註冊與使用的作業規範，及相關的權利與義務關係。

8. 用戶憑證管理中心的私密簽章金鑰只可用於用戶憑證與廢止憑證清冊的簽發，如有訊息加密或其他簽章的需求時，必須使用不同且獨立的私密金鑰。

(二) 管理及作業流程規範

1. 作業程序控管。

2. 人員控管。

3. 技術安全規範。

4. 憑證及憑證廢止清冊剖繪。

5. 稽核規範。

二、製卡中心規範

(一) 關於金鑰對產製規劃，有以下兩種方式：

1. 由卡片內部產生金鑰對。

2. 由卡片外部（HSM）產生金鑰對。

3. 綜合分析：

以資訊安全保障為前提，其金鑰安全為首要考量因素，故採取於卡片內產生金鑰對（如表 12）。

表 12：金鑰產製方法綜合評估

特性說明	**卡片內部產生金鑰對**	**卡片外部（HSM）產生金鑰對**
金鑰安全性	較高	略低
產製效能（製程可調性）	較低	較高
重覆製卡的可能	較不會	較可能

不可否認性	有	略低
修改憑證實務作業基準	不用	須修改並經審議委員會審核通過
建議	金鑰產製與個人化作業乃平行製程，如產能不足時，可增加設備或利用 New eID 系統調整整體作業流程，減少製卡中心負擔，使製卡中心之製程得以加快	強化相關安全配套機制

配合製發作業規劃採集中製發，於 New eID 卡片製程時於卡片內部產生金鑰對，New eID 集中製卡中心即應負責使之在內部安全產製用戶之金鑰對，而依據政府公開金鑰基礎建設憑證政策 1.3.6 規範，如憑證機構委託其他機構協助處理憑證作業相關事宜，應於憑證作業基準說明受託機構身分、管理方式及責任義務。

於此，製卡中心乃協助憑證作業相關事宜，憑證機構應於憑證實務作業系統內說明其身分並訂定作業程序等相關規範，因 New eID 採集中製卡，並由製卡中心負責控管 New eID 製證事宜。

(二) 卡管中心之職責

卡管中心關於憑證項目負責提供開通資料管理作業、提供解鎖管理作業以及卡片管理。

(三) 管理及作業流程規範

卡管中心應訂定符合憑證實務作業基準之作業規範、管理規範。

三、備援機制規劃

由於本案所需之全部運算資源均由內政資料中心來支應，因此就運算資源所需之硬體設備包含異地備援規劃，均配合內政資料中心所做的規劃，惟計畫所需之硬體密碼模組均需規劃異地備援或雙地均同時提供服務，另有關資料庫授權部分，如廠商規劃使用非 MS SQL 資料庫亦需同時規劃異地備援所需的資料庫系統所需之授權。

參、憑證效期及換發作業規劃

一、憑證效期規劃

本規劃憑證的效期，以不超過卡片金鑰載具的生命週期為原則，是以卡片製造日期（即卡面記載之製證日期）為憑證之效期起點，並以卡面記載之應換領日期為憑證之效期終點。

因憑證管理中心屬政府公開金鑰基礎建設之一環，其所簽發之憑證及私密金鑰的使用效期應符合政府公開金鑰基礎建設憑證政策對用戶公開金鑰及私密金鑰使用期限之規定，至多為 10 年，且考量憑證所使用之演算法安全強度及憑證內容的正確性，規劃憑證管理中心簽發之自然人憑證使用效期為 5 年，屆期可辦理 1 次憑證重新簽發，且憑證重新簽發作業僅適用於未被廢止之憑證。並定期檢視金鑰風險，未來若有變更金鑰演算法或更新 CA 金鑰時，將依據 ISMS 作業程序停止申請，並啟動大量換發程序以降低相關資安風險。

憑證重新簽發作業至少提供臨櫃辦理或線上憑證重新簽發等兩種辦理方式，相關作業程序與規定於憑證管理中心憑證實務作業基準中敘明。此外，若憑證年限屆滿且不得重新簽發時，為確保資訊的準確性，規劃民眾需至戶政事務所重新進行身分識別與鑑別，以取得新簽發之憑證，其憑證金鑰更換與憑證換發之相關辦理程序及規定亦於憑證管理中心憑證實務作業基準中敘明。

民眾於 New eID 發放時選擇停用憑證時，憑證效期不因此而有所遞延。

當發放 New eID 給 65 歲以上民眾時，其 New eID 卡片不設應換領日期。對於此類金鑰載具應換領日期超過 10 年的情況，其憑證在重新簽發 1 次且到期後，仍有簽發憑證之需求時，則必須換發新 New eID 卡片。

二、憑證換發作業規劃

民眾如已取得現行自然人憑證，於 New eID 換發時亦申請憑證，則原憑證將不廢止，可繼續使用到原憑證效期屆止，以避免對原應用系統衝擊過大。

(一) 初始個人密碼規劃

本案規劃採製發 New eID 卡片時即依民眾之申請，將憑證寫入晶片，並起算憑證效期。其憑證之初始個人密碼（以下簡稱 PIN2 碼），係申請人於領取 New eID 時，給予 1 份確認單，確認單上載有預設之用戶代碼。申請人須以該用戶代碼設定 PIN2 碼才可使用（即個人自訂密碼 8-12 數字碼）。

為配合憑證原則開通之規劃，並兼顧民眾資訊自主權，規劃民眾得選擇停(復)用或廢止憑證。

(二) 憑證屆期換發規劃

當用戶 New eID 效期屆期時，則 New eID 中的憑證效期亦同時屆期，此時必須辦理 New eID 換發，並依循 New eID 換發作業規範進行換發新 New eID 的憑證簽發作業。

憑證管理中心對於用戶 New eID 效期屆期後的憑證換發作業方式，須依循 New eID 換發作業及憑證管理中心憑證實務作業基準規範，採臨櫃辦理方式重新進行身分識別與鑑別，申辦換發新 New eID 及憑證簽發作業。

憑證管理中心在用戶申辦憑證重新簽發作業時，應提供用戶可採線上直接辦理或至戶政事務所辦理的方式。

(三) 憑證換發對象（※以下規劃僅為草案，實際情形須以內政部憑證管理中心憑證實務作業基準內容為準）

憑證實務作業基準規定申請人的年齡為 18 歲（含）以上，設有戶籍之國民，且未受監護宣告者。未來是否不限申請人年齡，尚待討論。

肆、 憑證實務作業基準修訂規劃

經評估本案建議採取擴充案之整合現行自然人憑證發證系統，依此修訂須符合 RFC 3647 架構之內政部憑證管理中心憑證實務作業基準，並審視政府機關公開金鑰基礎建設憑證政策（GPKI），相關規劃如下：

一、政府機關公開金鑰基礎建設憑證政策

配合憑證效期規劃，用戶之私密金鑰使用期限從原規定之 5 年可展期 3 年共 8 年，修正為 5 年可更換金鑰再用 5 年共 10 年，到期時民眾向憑證管理中心重新申請憑證，由註冊窗口對於重新申請憑證之用戶進行識別及鑑別。

二、費用規劃

簽發憑證無須收費，僅就載體部分收取工本費，相關費用以憑證管理中心公告為主。

三、識別和鑑別程序

(一) 個人身分鑑別之程序

配合 New eID 全面換發規劃，由戶政事務所受理 New eID 之申請，戶政事務所負責驗證申請人之身分與憑證申請相關資訊，是以，New eID 之負責窗口即屬戶政事務所，申請憑證實務作業基準所指自然人憑證之註冊窗口即為各直轄市、縣（市）戶政事務所。

(二) 憑證之金鑰更換

配合憑證效期最長使用期限為 10 年，用戶之私密金鑰使用期限應從原規定之 5 年，可展期 3 年共 8 年，修正為 5 年可更換金鑰再用 5 年，憑證使用期限到期時民眾應向憑證管理中心重新申請憑證，註冊窗口將對於重新申請憑證之用戶進行識別及鑑別。

四、金鑰使用期限

為考量資安兼具便民原則下，憑證效期 5 年不變，更換金鑰之後可再用 5 年，配合 GPKI 憑證政策仍維持 10 年內需至憑證註冊窗口重新認證機制。

五、金鑰產製

因應未來用戶 New eID 有更換金鑰演算法之情況，規劃應納入 ECC 演算法金鑰對之選項。

另建議密碼模組標準應使用通過 Common Criteria EAL 4+（含）以上或 FIPS 140-2 level 3 規範。

六、憑證申請程序

申請 New eID 並同意申請憑證，其無須先向戶政事務所進行身分確認，於民眾領取 New eID 時一併進行身分識別即可。當戶政事務所接受民眾申請憑證時，應先確認其未受監護宣告；如發證時民眾已受監護宣告，戶政事務所即逕行廢止憑證。嗣民眾領取領證確認書並確認憑證內容無誤或未有反對，即表示確認並接受憑證管理中心所簽發憑證。

有申請自然人憑證者，於製卡中心製發時，憑證資料寫入 New eID 之晶片內，且預設為啟用，未來得隨時辦理停（復）用、廢止自然人憑證。

因沿用現行自然人憑證管理系統，非我國籍者仍可申請僅具憑證功能之自然人憑證，非我國籍之申請者可依現行程序向註冊窗口申請。

現行線上申請或換發憑證，憑證實務作業基準要求申請人需選定個人用戶代碼及電子郵件信箱，惟 New eID 乃全面發放，恐面臨民眾反映其無電子郵件信箱，致申請程序有所障礙，考量電子郵件非每位民眾所必備，

而電子郵件之主要使用目的在於通知憑證申請者憑證相關訊息，建議修正為選定電子郵件信箱或其他可連絡之通訊方式。

七、卡管中心規劃

相關製發作業規劃上採集中製發，並於 New eID 卡片製程時一併寫入憑證金鑰對，且如上述於卡片內部產生金鑰對，是以負責驅動符記以產製用戶的金鑰對則由 New eID 製卡中心負責，於製卡中心以初始碼設定符記之初始 PIN 碼，驅動符記使之在內部安全產製用戶之金鑰對，而依據政府公開金鑰基礎建設憑證政策 1.3.6 規範，如憑證機構委託其他機構協助處理憑證作業相關事宜，應於憑證作業基準說明受託機構身分、管理方式及責任義務。

八、個人資料保護

現行憑證實務作業基準規定憑證內容記載用戶的中文或英文姓名，以及國民身分證統一編號或居留證號碼的後 4 碼，惟為加強憑證與 New eID 之關聯，應於憑證內記載 New eID 之卡片序號，故憑證實務作業基準之憑證內容建議增加記載 New eID 卡片序號之規定。

伍、New eID 晶片採用之中介軟體

建議依循 CSP（PKCS#11）標準，其具有跨平台之特性，APPLET（PKI）開發商應提供符合 CSP（PKCS#11）中介介面，再由 API 整合後提供標準介面，供未來各系統使用，亦可減少需用機關重複開發程式的成本。晶片廠商

須符合中介軟體所採用之規格並通過檢核，且須提供備援方案以確保規格。

一、中介軟體規劃

(一) 具備 PKCS#11 之介面。

(二) 具備金鑰產製、簽章、驗章、加密、解密、憑證載入等功能。

(三) 具備卡片識別功能。

二、中介軟體相容性規劃

(一) 使用 New eID 中介軟體之卡片識別功能，能判斷為 New eID 卡片或是自然人憑證卡片。

(二) 依卡片類別相容 New eID 中介軟體或自然人憑證中介軟體。

陸、 提供金鑰載具中金鑰對演算法及功能規劃

關於金鑰演算法採用 RSA 或 ECC 的安全性，於量子電腦興起，此兩類金鑰演算法都有可能遭到量子電腦破解。因此美國 NSA 決定準備要使用下一代密碼學標準「後量子密碼」（POST-QUANTUM CRYPTOGRAPHY，簡稱 PQC）來取代 RSA 與 ECC 金鑰演算法。美國 NSA 當局已經宣布未來將廢棄其最常被採用的 NSA SUITE B 密碼標準，包括過去常用的以下密碼標準組合：

一、SHA-256

二、AES-128

三、RSA WITH 2048-BIT KEYS

四、DH WITH 2048-BIT KEYS

五、ECDH AND ECDSA WITH NIST P-256

目前美國 NSA 建議若還未導入 ECC 演算法的廠商，可視情況不需於目前導入，可以在未來直接使用新的 PQC 密碼標準。

但是目前 PQC 標準尚待負責制定密碼標準的 NIST 組織作決定，NIST 組織預訂於 2022～2024 年間會宣布新的 PQC 密碼標準。

本案建議金鑰載具的金鑰演算法及功能規劃：

一、提供金鑰載具應同時具備 RSA 與 ECC 金鑰演算法，先採用 RSA 金鑰演算法使用 5 年，再更換為 ECC 金鑰演算法使用 5 年，憑證之金鑰載具採 2 組 RSA-2048 金鑰對與 2 組 ECC-P521 金鑰。

二、2 組 RSA 金鑰對及 2 組 ECC 金鑰對的用途分別為：用於數位簽章以及用於加解密或金鑰交換之用。其晶片內寫入根憑證、中繼憑證、2 組金鑰對之憑證。

三、提供金鑰對安全保護規劃，如金鑰對必須由晶片內部產生，私密金鑰不可匯出。金鑰運算操作應有密碼（PIN CODE）驗證保護。

四、提供憑證重新簽發及線上操作規劃。

柒、 結論

一、因應 New eID 憑證載體變更，應用機關之應用系統則須介接新卡片，其皆須調整或開發 AP，然為避免目前自然人憑證 6,300 多個線上憑證服務系統(機關內部或機關對

機關)造成過大負擔，建議採取擴充現行自然人憑證管理中心，為較妥適之作法。

二、憑證效期及換發作業須配合調整，如配合金鑰載具設定調整憑證效期,而換發作業規劃上為給予應用系統轉換過渡期,是以原憑證效期仍應保留到原效期屆止,較為妥當。

第捌章、先期作業期間 New eID 宣導資料規劃及製作

本規劃協助內政部辦理 New eID 換發事宜，完善 New eID 全面換發工作、後續營運及應用之各項規劃。提供全國民眾一個安全及可信賴的身分識別機制，讓新身分證之持有人能享受智慧政府便捷智能服務，達成倍增服務效能及永續透明治理之目標。

壹、廣宣主題

為維持專案廣宣的一致性與建立民眾的記憶點，並凸顯數位身分識別證作為數位政府基礎建設最後一哩，建議廣宣主要標語為「讓我們一同邁向智慧政府的創新服務紀元」，並依據廣宣形式與主題搭配適當之副標語，達到全民推廣目標。

貳、先期宣導資料成果

一、懶人包

為精簡政府單位的政策說明，方便民眾快速瞭解，透過政策懶人包，統一提供電子與平面媒體運用，以利政策說明之一致性，並讓民眾透過簡單的圖示快速認識並瞭解本次換發之數位身分識別證。

懶人包主要目的是讓民眾可以透過圖示快速認識數位身分識別證，瞭解數位身分識別證與現行身分證之差異，並就可能引發民眾疑慮之部分進行釐清。

二、宣傳海報

為推廣宣傳數位身分識別證效益並提醒民眾相關換發作業應備文件或流程，規劃數款海報主題並委託設計師繪製完成，以供內政部後續印製並發送予各地戶所。

宣傳海報主視覺為藍綠色系之數位身分識別證示意圖，並依據個別主題搭配標語。其宣導海報主題包括：「New eID 常見問與答」、「New eID 功能更升級」、「New eID 掛失完全攻略」及「New eID 兼具數位簽章，功能更多元」等。

第玖章、建置及換發期間 New eID 專屬網站、宣導資料及戶所人員教育訓練課程規劃

為使全國民眾瞭解本次 New eID 換發方式並認識 New eID，而有建置網站並進行廣宣之必要。另為使戶政事務所人員能順利進行換發作業，並向民眾說明 New eID 之使用方式，亦有對戶所人員進行教育訓練之必要。依據前述之需求歸納 3 點專案目標如下：

一、認識 New eID（主要對象為民眾與戶所同仁）。

二、換發方式說明（主要對象為民眾與戶所同仁）。

三、釋疑澄清。

壹、 New eID 專屬網站規劃

本案為我國身分證數位化之重大里程，規劃於內政部入口網，建置專屬的 Banner 連結（如下圖所示），以利民眾查詢。

圖 8：內政部入口網連結示意圖

為達政策廣宣及線上線下整合之綜效，網站規劃與功能設計說明如下（暫定）：

圖 9：網頁示意圖

一、數位身分識別證說明

詳細介紹數位身分識別證的換發緣由、卡面及晶片登載資訊、使用方式及未來應用。

二、最新消息

有關數位身分識別證換發的最新消息，包括實際換發數字統計、新聞發布與釋疑.....等。

三、換發流程說明

提供數位身分識別證的換發流程圖，便於民眾理解。

四、線上申請

提供民眾可以在線上提出申請換發數位身分識別證與列印晶片各區資料。

五、常見 Q&A

以民眾常見的 5 大問題為主，並輔以懶人包圖示。

六、常用功能

包含「如何申請」、「換發單位查詢」、「問答集」、「影音專區」、「資料下載」、「聯絡我們」及「無障礙網頁」等功能。

七、其他功能說明

(一) 社群連結：於網頁右方設置內政部 New eID Line@。

(二) 行動身分證連結：設置行動身分證 APP 下載連結之 QR code，方便民眾掃描下載。

(三) 共同行銷：網頁下方為「政府單位資訊交換連結專區」，可進行雙方 banner 連結，共同行銷政府政策。

貳、New eID 廣宣策略分析

為兼顧預算與各族群的需求，建議採取「點、線、面」的整合行銷推廣方式，主要說明如下：

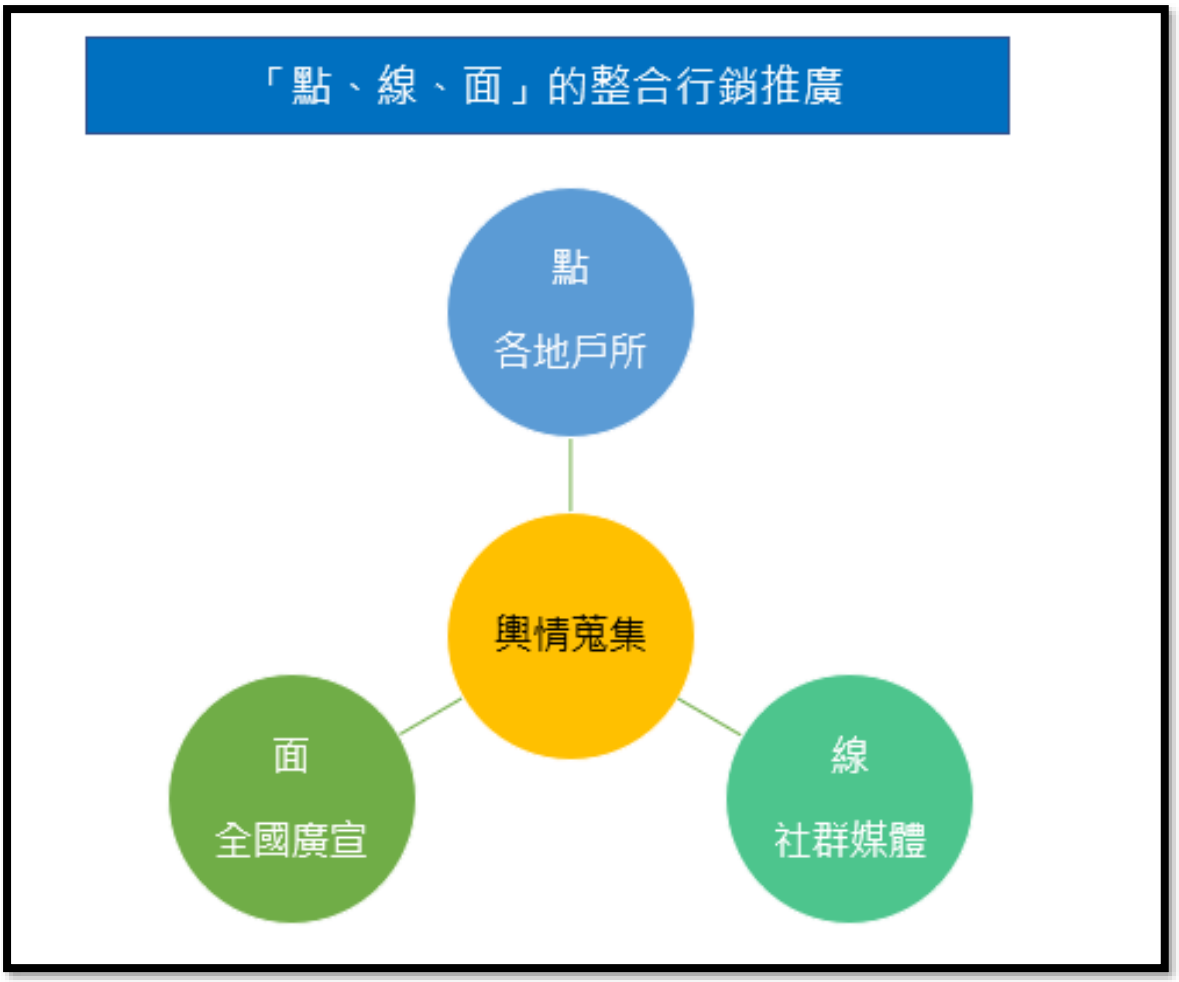


圖 10：「點、線、面」的整合行銷推廣方式

一、「點」→各直轄市、縣（市）戶所

各直轄市、縣（市）戶所為民眾第一線接觸點，將提供下列資源供戶所同仁運用：

(一) 公版宣導海報與摺頁 DM。

(二) 公版全國宣導影片。

(三) 戶政人員教育訓練手冊。

(四) New eID 主要 Q&A。

(五) 系統障礙排除 SOP。

(六) 跑馬燈文字建議。

(七) 網頁連結 Banner 設計。

二、「線」→社群媒體

根據 105 年 Nielsen 的網路使用行為接觸率調查，「20~59 歲」臺灣主要的消費群體「網路接觸率」已超越電視（網路 89.7%、電視 86.5%），躍居成消費者媒體接觸率第一的媒體別，建議操作方式如下：

(一) 搭配內政部「LINE@」及臉書專頁發布 New eID 相關訊息。

(二) 拍攝 New eID 的換發與使用體驗影片，並在社群媒體散布，讓民眾瞭解換發方式。

(三) 製作懶人包、設計圖稿或串聯其他政府機關社群小編帶動申辦換發 New eID 之風潮，快速讓民眾瞭解 New eID 使用方式，並進行釋疑。

三、「面」→全國廣宣

依前述的各直轄市、縣（市）戶所「點」與社群網絡構成的神經網絡「線」，進一步推升到全國廣宣的「面」，達到點、線、面合一的全方位廣宣綜效，建議方式如下：

(一) 善用行政院公益託播管道與地方政府的各式公務行銷管道（網站連結、APP 推播、公播頻道、村里長辦公室）。

(二) 拍攝 New eID 宣導廣告與動畫並於全國性電子媒體播放。

(三) 錄製 New eID 電台宣導廣告，於全國性廣播電台播放。

(四) 於 6 都的重要大眾運輸工具張貼 New eID 宣導廣告。

(五) 於臺鐵與高鐵車廂內的跑馬燈刊登換發提醒文字。

(六) 於全國性報章雜誌刊登 New eID 宣導廣告或專題報導。

參、108-109 年廣宣重點期程規劃

108 年先期作業期間與換發作業籌備期間，先製作政策懶人包、4 大換證方式與主要 Q&A 等廣宣 DM 與跑馬燈文字，透過內政部網站、網路社群、各直轄市、縣（市）政府戶政事務所、公務行銷（公益託播管道）.....等，進行宣導，協助民眾釋疑。

因應 110 年 1 月開始部分縣市試行作業，為使作業順利，須提前進行相關宣導，故區分為「換證預告期」、「樣張公布說明期」、「換證方式與應備資料宣導期」、「全面換證執行期」。

肆、戶所人員教育訓練課程規劃

一、目標

(一) 透過本課程使全國戶所人員認識 New eID，並據以辦理本作業及後續戶政等相關政府業務。

(二) 透過本課程使全國戶所人員瞭解本作業執行上應注意事項，以提升本作業執行效率並減少民眾抱怨情形。

二、規劃舉辦方式

(一) 實體教育訓練

為縮短教育訓練時程，且達到快速擴散效應，讓全國各直轄市、縣（市）戶所人員能在最短的時間內瞭解數位身分識別證的作業流程與使用。

(二) 線上教育訓練

為便利戶所人員隨時學習，並能即時更新最新的宣導資訊，搭配專案官網同步增設「數位身分識別證教育訓練專區」，透過網站影音學習，課程結束即進行線上測驗，首次通過測驗者可登錄公務人員學習時數（實體與線上課程擇一登錄）。

表 13：戶所人員教育訓練課程表（暫定）

換發作業訓練課程		
時間	課程名稱	課程重點說明
09：00-10：30	數位身分識別證換發作業說明	為讓戶所人員了解換發作業時程、領取應備文件及其他各項配合事項。課程重點包含： ● 換發作業時程 ● 申請換發方式 ● 相片規格與注意事項 ● 領取數位身分識別證應備文件與檢核方式 ● 辦理到府服務應注意事項
10：40-11：40	數位身分識別證（含晶片）基本介紹	了解數位身分識別證(含晶片)之基本內容。
11：40-12：00	意見交流	開放戶所人員提問，協助蒐整未來換發作業可能面臨問題，並作為行銷推廣或

		釋疑澄清重點之參考。
上機實作訓練課程		
09：00-10：30	系統功能說明	提供戶政人員受理申請作業時，使用系統完成資料核對與建檔登錄。課程重點包含： ● 系統功能與操作說明 ● 審核結果註記方式
10：40-11：40	數位身分識別證換發系統作業流程介紹	協助戶所人員受理民眾申辦時，能夠迅速且簡易地答復民眾對於數位身分識別證換發系統基本功能與常見問題之詢問。課程重點包含： ● 掛失補發流程 ● 忘記密碼處理方式 ● 戶所人員晶片各區讀取方式 ● 數位身分識別證使用疑義諮詢管道 ● 數位身分識別證換發系統介面應用 ● 數位身分識別證各項資料更新與換發之處理流程
11：40-12：00	意見交流	開放戶所人員提問，協助蒐整未來換發作業可能面臨問題，並作為行銷推廣或釋疑澄清重點之參考。

第拾章、New eID 空白卡（含晶片）管理及製發安全控管

壹、目標

確保 New eID 之空白卡（含晶片）採購、印製及運送之安全及品質，且採取安全管控的方式確保印製階段無資料外洩。

貳、作業程序

一、製卡中心辦理空白卡（含晶片）之採購作業

(一) 採購作業

1. 空白卡（含晶片）採購作業

(1) 為確保空白晶片卡之安全性，承作卡片之生產廠於生產卡片時須取得 EMV（Europay, Mastercard, and Visa）或 PCI-DSS（Payment Card Industry Data Security Standard）或其他相同等級之規範認證，以確保空白卡產製及運送之安全性；且於執行空白晶片卡生產期間，採購方得隨時至卡片生產廠辦理查驗，廠商不得拒絕。

(2) 採購之空白晶片卡規格應符合本部所訂定之規格，並依規定製作卡體防偽措施，且晶片內容須已完成以下步驟：

A. 提供之應用程序至少需包含 eID 及 ePKI 等功能，即包含 PKI 及其他應用於本案 4 區（即「戶籍地區」、「公開區」、「加密區」、「自然人憑證區」）資料使用的相關應用程序。

B. 寫入晶片資料包含：Answer To Reset （ATR）與

Card Production Lifecycle Data （CPLC）；ATR History bytes 需根據買方需求做設定；CPLC 須包含晶片廠商資訊、晶片序號、生產批號等晶片相關資訊。

(3) 設定卡片出廠金鑰，卡片金鑰須以約定之演算法計算並設定至卡片。

(4) 完成空白晶片卡整批生產後，需產製卡片資料檔，其中卡片資料檔須包含晶片序號及 CPLC 等卡片資料，且卡片資料檔須以約定之演算法加密保護，並於交貨同時提供此資料檔。

2. 耗材採購作業

(1) 製卡中心於製發過程中有製發 New eID 之耗材需求時，將由製卡中心開始辦理耗材之採購作業。

(2) 採購內容

A. 管制性耗材：係指製發 New eID 晶片卡片之必要原料，如空白 PC 晶片卡片、彩色列印耗材等。

B. 非管制性耗材：係指為輔助製發流程控管之原料，如信封、紙張、條碼碳帶、印表機墨水。

3. 製卡中心針對空白卡（含晶片）採購內容之確認應建立內部審查程序，以確保採購內容無誤。

二、卡廠辦理空白卡（含晶片）生產及運送作業

(一) 生產作業

1. 卡廠於寫入晶片資料時應包含 Answer To Reset（ATR）、Answer to Select（ATS）及 Card Production Lifecycle Data （CPLC）。ATR History bytes 應符合內政部需求完成設定；CPLC 應包含晶片廠商資訊、晶片序號、生產批號等晶片相關資訊。

2. 卡廠應於空白卡（含晶片）以內政部與製卡中心約定之演算法計算並設定卡片出廠金鑰，並應於整批生產後產製卡片資料檔，該資料檔包含晶片序號及 CPLC 等卡片資料並應以約定之演算法加密保護，並於交貨同時提供此資料檔。

3. 卡廠應依內政部規定之空白卡（含晶片）卡體各層皆為聚碳酸酯（Polycarbonate, PC），且依規範製作卡面之各項防偽措施。

(二) 運送與包裝作業

卡廠於製作完成符合採購單規格之空白卡（含晶片）後，於運送前應採用運送金鑰(Transport Key)進行加密保護，該金鑰採分段分持原則，應以不同途徑由安全傳遞至製卡中心，以確保空白卡運輸過程安全無虞，防止未經授權之存取。製卡中心將運送金鑰組合後方可存取空白卡，並取得其控制權。製卡中心確認金鑰真偽後，即可進行金鑰交換作業，由製卡中心產製之新金鑰替換卡廠之運送金鑰，此時，空白卡之控制權才由卡廠移轉至製卡中心(即為洗卡程序)，卡廠應依下列方式進行空白卡包裝及運送。

1. 包裝

包裝應符合防潮、防水、防破損及防碰撞等基本包裝防護規定，另需確保 PC 卡緊密置放於盒中不會鬆動摩擦。

(1) 卡片裝盒方式

A. 卡廠應以 250 張或 500 張卡片為單位將卡片裝於卡盒內。

B. 卡盒需有封裝防潮，每盒外包裝需標註盒號、生產批號、產品名稱、作業系統名稱、PC 卡數量及製造日期等資訊（可由盒號查詢前項交貨資料之晶片 ID 資訊）。

(2) 卡片整批裝箱方式

A. 卡盒應裝於堅實之箱匣內，並以適當保護材料填實，以防遞送途中，物與物或物與箱壁間之摩擦或碰撞。卡片之箱匣外應以彌封條加以彌封，以加強控管。

B. 箱上應有識別條碼，此識別條碼之編碼應同時可為人工判讀並合於標準條碼型式。

C. 若點收人員於開啟前發現彌封條已破損時，應立即通報上級主管加以處理。

2. 運送

(1) 運送規格：採全程安全運送規格。

(2) 運送方式：

A. 車輛運送

(a) 保全車輛：運送全程需在雙重控制下進行，運卡車輛不可有任何運送物品之標示或商標，卡片包裝需隨時有人看管，除非是在保全區域，如在運送期間臨停，承運人須確保卡片包裝之完整性。

(b) 非保全車輛：以非保全車輛運送，除運卡車輛外，需有未運卡之隨行車輛，在運送期間內需有雙重控制，且不得無人看管，車輛必須配備電話或與保安雙向無線電聯繫，運卡車輛不可有任何運送物品之標示或商標，需直接交付（點對點）。

B. 飛機運送

卡片包裝必須保管在上鎖或密封的容器，應以載送貴重物品之規格載送，不允許合併運送，嚴禁手提攜帶，從出貨點到目的地位置之間的運輸不可間斷，送達之目的地必須能夠安全處理卡片包裝，如果在航空運輸過程中途停止，必須確保卡片包裝的完整性，如果在飛行之前，期間或之後需要任何地面存儲，則必須是在授權人員始得進入之安全區域。

C. 船舶運送

卡片包裝必須保管在上鎖或密封的容器，並使用集裝箱裝運，不允許合併運送，亦嚴禁手提攜帶，從出貨點到目的地位置之間的運輸盡量不間斷，須立即安排從碼頭出發和接送。

(3) 出貨

A. 卡廠出貨應檢附出貨單，其內容及注意事項如下述：

(a) 出貨單內容須包含：品名、規格、數量及批號，並提供 QR Code 條碼，條碼內需有上述之出貨單內容。

(b) 出貨前須由權責人員確認經包裝之空白卡與製卡中心與出貨單內容一致。

(c) 運送單位運送至製卡中心。

B. 運送單位應由專屬運送人員以專車分別從卡廠統籌分配至製卡中心之卡片存放區。

C. 每個轉手階段之負責人，無論是裝貨、卸貨，收件人均必須明確驗貨，雙方簽認並詳細記載於管制紀錄中。

(4) 交貨

A. 驗收標準

(a) 製卡中心之專門人員應以相對應的防偽檢測設備，採抽驗方式檢測卡片品質。

(b) 製卡中心之專門人員從每個空白卡(含晶片）之包裝中抽取每包裝張數之 2%數量。

(c) 抽驗中的卡片只要含有一張係為不合品質之空白卡（含晶片），該空白卡（含晶片）之包裝即驗收不合格，應整個包裝退回卡廠；並由製卡中

心之專門人員製作驗收不合格報告,檢送報告回送給卡廠並且為登記。

B. 完成交貨

製卡中心於空白卡（含晶片）存放區，經專門人員負責卡片及卡片資料檔之點、驗收後，並於管制紀錄單中，簽名及填寫日期始完成交貨之程序。

三、New eID 製程安檢作業

(一) 卡廠之空白卡（含晶片）安檢作業

1. 卡廠須對印製完各項防偽措施之空白卡（含晶片）進行品質檢驗，由卡廠印製人員以相應防偽設備觀察其防偽措施是否有印製不良之情況（如無反光情況）。

2. 不良空白卡（含晶片）蒐集達一定數量，依規定進行銷毀程序。

(二) 製卡中心製程安檢作業

1. 空白卡初始化作業人員將空白卡（含晶片）放置於機台上前，應以相應防偽設備觀察其防偽措施是否有印製不良之情況（如無反光情況）。

2. 空白卡（含晶片）品質若有問題，則視為壞卡，並依壞卡控管作業程序辦理。空白卡（含晶片）品質若無問題，則續行空白卡初始化程序。

3. New eID 製發後，由製卡作業人員透過讀卡設備進行卡片及晶片品質檢測，以確認卡面及晶片資料一

致性，且卡片與卡機須定期依照成卡品質標準及控管規範訂定之標準進行檢測。成卡控管檢查項：

(1) 相片是否有污損。

(2) 證卡上文字是否清晰可見。

(3) 印製之資料是否完整呈現。

(4) 依照防偽等級採對應之驗證方法。

4. 倘成卡品質不佳，則視為報廢卡，製卡作業人員應依報廢卡控管作業程序辦理。

5. 印製設備廠商需提供定期檢測服務，以儀器確認 PC 卡材質、雷射雕刻及彩印效果，並調整機器參數，以符合成卡品質要求。

四、產品庫房安全管理

所有卡片及耗材管制作業系統流程中使用之相關表單除人工詳實填寫外，須於生產管理系統確實登錄，便於日後稽查管理、管制、統計及產製相關報表，相關文件保存至少 10 年，以備查驗。

(一) 庫房檢核管理:庫房人員根據生產管理系統確認卡片數量後，進行空白卡（含晶片）、半成卡、成卡、壞卡、報廢卡數量抽查作業，並分為每日、每月之檢核。

(二) 卡片出入庫管理

1. 入庫管理：空白卡（含晶片）、半成卡、成卡、壞卡、報廢卡之入庫作業，應由作業人員比對生產管理系統對應之卡片數量以確認。

2. 出庫管理：空白卡（含晶片）、半成卡、成卡、壞卡、報廢卡之出庫作業，作業人員應依照作業程序持申請單至庫房檢核後，依申請數量領取。

五、耗材安全管制

(一) 耗材入庫管理

1. 新採購之耗材入庫

(1) 廠商出貨耗材應檢附出貨單，出貨單內容須包含品名、規格、數量及批號，並提供 QR Code 條碼，條碼內需有上述之出貨單內容。

A. 檢驗項目包括：廠牌、型號、規格、進廠數量。

B. 品管事務組人員品檢後應填寫「耗材紀錄表」。

C. 耗材紀錄表之文件保管：品管事務組人員填妥文件後，應將文件送交檔案組保存，以備查驗。

(2) 耗材庫房人員應將耗材置於相對應之存放位置。

2. 已領取未使用完畢之耗材

(1) 由卡片作業人員確實點驗並填具耗材繳回申請單。

(2) 卡片作業人員應將申請單併同耗材送交耗材庫房人員，並於當場清點繳回之耗材，數量正確無誤，且至生產管理系統更新耗材繳回申請單處理情況及數量。

(二) 耗材出庫管理

1. 由卡片作業人員至生產管理系統填寫耗材申請單，並持申請單至耗材庫房領取。

2. 耗材庫房人員應比對申請單內容與生產管理系統上之資訊是否一致，確認無誤並檢核數量後，交予卡片作業人員，且兩者交接耗材時應當場清點，並於管制紀錄進行登記。

六、廢料及廢卡控管

(一) 廢料控管

1. 卡片作業人員製發卡片過程中，使用之耗材產生出無法再使用或廢棄之部分，稱之為廢料。

2. 由卡片作業人員將廢料集中於各區之廢料區，於例行工作日結束前，將廢料區之物送至廢料銷毀區。

3. 當銷毀區庫存達一定數量時，委請清潔公司將廢料送至焚化爐或合格之回收單位，並應製作管制紀錄及留存。

(二) 壞卡控管（品質不佳之空白卡）

1. 初始化作業人員應將壞卡置於壞卡蒐集處，並於生產管理系統登記壞卡入庫申請單，內容應包含：記錄檢核人員、空白卡初始化作業人員、檢核日期、檢核地點、貨品名稱、貨品檢核數量及壞卡原因。

2. 銷毀

(1) 壞卡庫房人員應定期執行壞卡銷毀，執行銷毀時，應比對確認壞卡銷毀申請單與壞卡之數量。

(2) 壞卡庫房人員會同管制人員進行清點數量後，送交卡片銷毀單位並依銷毀程序進行，並應製作管制紀錄及留存。

(三) 報廢卡控管（印製完成但品質不佳之成卡）

1. 報廢卡作業人員應將報廢卡置於報廢卡蒐集處，並於生產管理系統填寫報廢卡入庫申請單，內容應包含：紀錄檢核人員、空白卡初始化作業人員、檢核日期、檢核地點、貨品名稱、貨品檢核數量及報廢原因。

2. 報廢卡作業人員應先於實體卡片接觸式與非接觸式晶片位置進行實體破壞，防止惡意用途。

3. 銷毀

(1) 報廢卡庫房人員發現報廢卡數量高於標準時，應進行報廢卡銷毀流程。

(2) 報廢卡庫房人員應確實比對報廢卡銷毀申請數量，會同管制人員確實清點數量後，送交卡片銷毀單位進行銷毀，並應製作管制紀錄及留存。

七、廢料及廢卡銷毀程序

(一) 由製卡中心庫房人員確認廢料及廢卡銷毀申請單與生產系統資訊相同。

(二) 會同管制人員送交於卡片銷毀單位，卡片銷毀人員須清點廢料及廢卡裝箱之數量，並於裝箱上標註總數以核對銷毀數量。

(三) 銷毀人員將裝箱之廢料及廢卡裝配上車，前往銷毀廢料及廢卡之廠址（如焚化廠），辦理銷毀全程應拍照及錄影存證，並須記錄銷毀排程單及後續銷毀程序之文書資料並歸檔。

八、內政部實地稽核作業

(一) 內政部對製卡中心之稽核作業

1. 內政部得向製卡中心為不定期稽核作業，以確保具體執行 New eID 製發之作業程序。

2. 內政部得由代表人至製卡中心稽查製卡中心與卡廠溝通之文書記錄、空白卡（含晶片）紀錄表、與卡廠間成立之運送契約等相關文書。

3. 製卡中心倘有不符合規定（如未為記錄、不提供資料等），內政部以書面通知製卡中心改善事由，收到書面通知後之 7 日內應為補正。

4. 倘製卡中心逾期未補正，內政部得以再次以書面通知續行改善，第二次書面通知後之 7 日內怠於補正或未達補正標準，依契約規定辦理。

(二) 內政部對卡廠之稽核作業

1. 內政部得向卡廠為不定期稽核作業，以確保卡廠確實執行 New eID 製發之作業程序。

2. 內政部得由代表人至卡廠稽查製作空白卡（含晶片）之作業流程與製卡中心溝通之文書記錄、空白卡（含晶片）紀錄表、與製卡中心間成立之運送契約等相關文書。

3. 卡廠倘有不符合規定（如未符合作業流程、未為記錄、不提供資料等），內政部以書面通知卡廠改善事由，卡廠收到書面通知後之 7 日內應為補正。

4. 倘卡廠逾期未補正，內政部得以再次以書面通知卡廠續行改善，第二次書面通知後之 7 日內怠於補正

或未達補正標準，內政部得請製卡中心更換其他卡廠。

第拾壹章、各項標準作業程式（SOP）－New eID 全面換發作業

壹、目標

規劃全面換發國民身分證作業換發期間應遵行事項，俾利辦理機關及民眾遵循。

貳、辦理機關

在中央為內政部；在直轄市為直轄市政府及所轄戶政事務所；在縣（市）為縣（市）政府及所轄戶政事務所。

參、數位身分識別證（New eID）全面換發作業

一、換發對象

全面換證對象係在國內設有現戶戶籍者約 2,359 萬人，但不包括矯正機關收容人，矯正機關收容人於出矯正機關後，再向戶政事務所申請 New eID。出境戶籍遷出國外人口，辦理遷入登記時，同時向戶政事務所申請 New eID。

二、換證規劃

申請換領 New eID 之方式包含「網路申請」、「排定地點申請」、「臨櫃申請」及「到府服務」等 4 種。其中網路申請規劃可指定任一戶政事務所領證，為維護戶政事務所辦理案件之品質，系統會顯示當日可受理之非戶籍地案件名額，如當日名額已滿，民眾可選擇其他日期之名額或選擇其他戶政事務所領證。至「排定地點申請」受理戶籍地案件，「臨櫃申請」及「到府服務」開放非戶籍地民眾申請。

(一) 戶政事務所通知換證

1. 換發前準備作業

排定通知換證期程：依所轄村（里）、鄰人數，排定換證期程、人員及地點。

2. 通知換證作業

(1) 戶政事務所應因地制宜自行排定換證期程及地點。

(2) 最遲應於排定換證日期前 15 日，辦理下列事項：

A. 張貼換證公告於村（里）辦公處公告欄公告之。

B. 按戶分送換證通知單、換證申請書、收件證明、換證委託書、國民身分證數位相片繳交方式及相片規格等資料，其中換證申請書之張數依戶內換證人口數發給，其餘文件均為 1 戶 1 張。

(3) 請民眾依戶政事務所通知的時間選擇上網申請、至戶政事務所排定地點或臨櫃送件。有特殊情形如身心障礙、65 歲以上行動不便、重大傷病住院或在家療養不便外出、其他行動不便，且無合適人選得委託代為送件，經受理申請之戶政事務所認有必要時，得派員至申請人指定地點到府受理 New eID 之申請(由各縣市視其人力調配及資源情況決定提供服務之時機)。

(4) 對逕遷戶政事務所者，戶政事務所仍需排程換證，但得毋庸進行換證通知，當事人可自內政部網站查詢換證時程後，向戶籍地戶政事務所領取換證通知單、換證申請書等文件，並向戶籍地戶政事務所申

請換證，不得異地申請換證。

3. 全面換發國民身分證通知單應敘明事項：

(1) 欄位說明：主要內容包含戶長及戶內換證人口姓名、戶籍地址、申請方式及受理時間地點、網頁申請之連結 QR code 及注意事項。

(2) 上開注意事項應包含以下內容:申請人、申請方式、戶政事務所排定地點、臨櫃申請應備文件、網路申請程序、外文姓名填寫注意事項、民眾聯絡資訊填寫注意事項、用戶代碼解鎖方式注意事項、委託送件注意事項、各年齡區間申請 New eID 之卡片應換領日期、自然人憑證申請規定及效期說明、規費繳交之說明以及領證注意事項等。

(二) 受理申請作業

民眾收到換證通知單後,申請人應親自依戶政事務所通知的時間選擇上網、至戶政事務所排定地點或臨櫃申請。有下列特殊情形且無合適人選得委託代為送件,經受理申請之戶政事務所認有必要者：身心障礙者、65 歲以上行動不便者、重大傷病住院或在家療養不便外出者或其他行動不便者。

1. 網路申請

(1) 申請資格：

A. 本人。

B. 未滿 14 歲者，法定代理人為申請人。

(2) 申請地點：內政部指定網站。

(3) 申請流程：

A. 掃描換證通知單 QR code 或輸入網址，登錄網站後可擇以下任一方式申請：

(a) 使用自然人憑證申請。

(b) 使用健保卡申請。

(c) 使用國民身分證申請。

B. 選擇領證之戶政事務所系統會顯示當日可受理非戶籍地案件名額，如當日名額已滿，民眾可選擇其他日期之名額或選擇其他戶政事務所領證。

C. 資料送出後，畫面顯示申辦成功。

2. 排定地點申請

(1) 申請資格：

A. 本人。

B. 未滿 14 歲者，法定代理人為申請人。

(a) 法定代理人申請時，須另檢附其國民身分證或其他身分證明文件、印章（可簽名）。

(b) 如法定代理人之一方，無法申請時，應出具換證同意書或換證委託書，由另一方代為申請。

C. 委託送件時須另檢附受託人國民身分證或其他身分證明文件、換證委託書、印章（可簽名）。

(2) 申請地點：戶政事務所排定地點集體收件：如學校、村（里）鄰辦公處、社區活動中心等場所。

3. 臨櫃申請

(1) 申請資格：

A. 本人。

B. 未滿 14 歲者，法定代理人為申請人。

(a) 法定代理人申請時,須另檢附其國民身分證或其他身分證明文件、印章（可簽名）。

(b) 如法定代理人之一方，無法申請時，應出具換證同意書或換證委託書，由另一方代為申請。

C. 委託送件時須另檢附受託人國民身分證或其他身分證明文件、換證委託書、印章（可簽名）。

(2) 申請地點：向任一戶政事務所申請。

4. 到府服務(由各縣市視其人力調配及資源情況決定提供服務之時機)

(1) 申請資格：

有下列特殊情形且無合適人選得委託代為送件，經受理申請之戶政事務所認有必要者：身心障礙者、65 歲以上行動不便者、重大傷病住院或在家療養不便外出者或其他行動不便者。

(2) 申請地點：向任一戶政事務所申請，戶政事務所得派員至申請人指定地點受理申請。

(3) 應備文件及申請流程：同排定地點申請。

5. 申請相關注意事項：

(1) 全面換證期間舊證遺失之補證方式：已收到申請換證通知單者，可網路申請補領新證，但申請前舊證應先辦理掛失作業，另領證時再繳納補證規費，非戶籍地申請補證案件亦受受理戶所當日得網路申請非戶籍地案件最高人次限制；尚未收到申請換證通知單者，或有急需身分證明文件者，須親至戶所臨櫃申請補證，並依需求申請臨時證明書。另當事人臨櫃向戶所辦理補領新證時，不可委託申請。

(2) 如不申請自然人憑證，可於換證申請書上勾選「不申請自然人憑證」欄位，New eID 將不會寫入自然人憑證，未來如須使用自然人憑證，須付費換領 New eID 或另付費申請憑證。

(3) 申請 New eID 時，可於換證申請書勾選是否附加自然人憑證，說明如下：

A. 選擇附加自然人憑證者，New eID 能使用自然人憑證，無須再支付自然人憑證費用。

B. 選擇不附加自然人憑證者，新證不能使用自然人憑證，但申請人可於領證時，再付費申請單張自然人憑證。

C. 申請人亦可待未來需使用自然人憑證時，再付費換領新證附加自然人憑證之新證或申請單張自然人憑證。

(4) 失蹤人口應先請當事人至警察機關辦理撤尋後，再申請 New eID。

(5) 換證委託書、換證同意書表單遺失或不敷使用時，

可自內政部戶政司全球資訊網（https：//www.ris.gov.tw）下載空白表單，或至戶政事務所索取。

(6) 繳交或上傳數位相片，當事人有顏面傷殘、患重病、植物人及其他特殊情形等，經戶政事務所許可者，New eID 得免列印相片，但仍須繳交數位相片。

6. 委託送件

全面換證委託送件時，除應檢附本人申請之應備文件外，另須檢附受託人國民身分證或其他身分證明文件及委託書。

7. 未滿 14 歲未成年子女之父或母單獨一方申請

未滿 14 歲未成年人之法定代理人若無法一同到場申請時，得由一方為之，他方應出具單獨申辦同意書或換證委託書。

8. 戶政事務所進行申請資料登錄及審核無誤後送 New eID 管理系統，依集中製證產能控管，批次傳送定量換證申請案，並依當事人最新戶籍資料傳送製卡中心製卡。

(三) 戶政事務所 New eID 點收

New eID 送達戶政事務所（中心所），中心所再通知區所、辦公室、辦公處及辦事處派員至中心所領取並點收 New eID。

(四) 戶政事務所進行品管檢驗 New eID 作業

1. 戶政人員自 New eID 管理系統下載領卡名冊，依照名冊順序，清點及檢查 New eID。

2. 戶政事務所發現 New eID 版面或晶片有瑕疵時列為瑕疵卡，應依規定之方式打洞截角作廢，於系統登錄作廢情形，並申請重製 New eID，重製完成前，毋須通知申請人領證。

3. 戶政事務所品管檢驗 New eID 時，系統檢核為受監護宣告者，辦理廢止自然人憑證，至有下列情事者，應依規定之方式打洞截角作廢，並於系統登錄作廢情形：

   (1) 民眾有出境戶籍遷出、死亡、受死亡宣告、廢止、撤銷戶籍登記者。

   (2) 民眾因舊證遺失或辦理戶籍登記同時須換發國民身分證已轉成例行製證者，由系統檢核不得重複請領。

4. 戶政事務所人員檢查無誤後，於系統執行領證通知作業，並依民眾指定領證通知方式通知當事人於排定時間領取 New eID。

(五) 戶政事務所核發 New eID

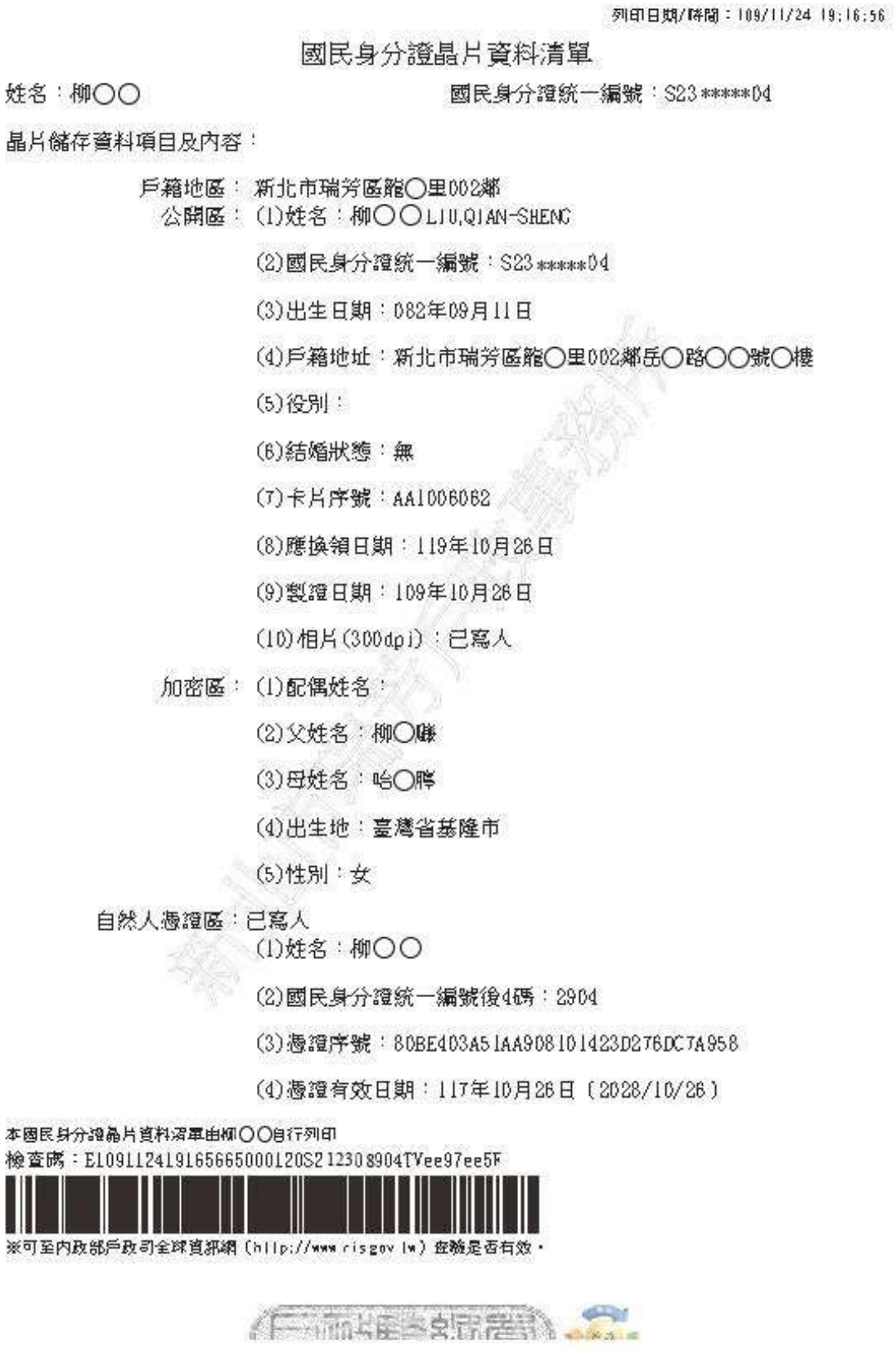
1. 戶政人員核對本人應備文件、戶籍資料、並再次確認晶片內容是否為最新，如發現 New eID 版面或晶片有瑕疵，應立即打洞截角回收 New eID，並上系統申請作廢及重製 New eID。

2. 將裝有 New eID 信封交給申請人現場打開，請申請人檢查 New eID 外觀及確認領證確認書內容無誤後，

於存根聯簽名或蓋章，New eID 及領證確認書(收執聯)由申請人攜回，舊證由戶政事務所截角後收回。

3. 提醒申請人，部分公私立機關若尚未完成系統修正，致無法讀取晶片資料，或申請人不願需用機關（構）使用晶片讀取其個人資料者，可向戶政事務所或自行上網申請國民身分證晶片資料清單，搭配 New eID 作為身分證明文件。惟 New eID 掛失後，其國民身分證晶片資料清單暫時停止效力。

4. 國民身分證晶片資料清單上具浮水印、騎縫章及驗證序號供查驗資料內容有無被竄改，同現行電子戶籍謄本，使用機關可自內政部戶政司全球資訊網（https：//www.ris.gov.tw）查驗是否有效，樣式如圖 11。



列印日期/時間：109/11/24 19:16:56

國民身分證晶片資料清單

姓名：柳○○　　國民身分證統一編號：S23*****04

晶片儲存資料項目及內容：

戶籍地區：新北市瑞芳區龍○里002鄰

公開區：(1)姓名：柳○○LIU,QIAN-SHENG

(2)國民身分證統一編號：S23*****04

(3)出生日期：082年09月11日

(4)戶籍地址：新北市瑞芳區龍○里002鄰岳○路○○號○樓

(5)役別：

(6)結婚狀態：無

(7)卡片序號：AA1006062

(8)應換領日期：119年10月26日

(9)製證日期：109年10月26日

(10)相片(300dpi)：已寫入

加密區：(1)配偶姓名：

(2)父姓名：柳○雄

(3)母姓名：哈○聘

(4)出生地：臺灣省基隆市

(5)性別：女

自然人憑證區：已寫入

(1)姓名：柳○○

(2)國民身分證統一編號後4碼：2904

(3)憑證序號：80BE403A51AA908101423D276DC7A958

(4)憑證有效日期：117年10月26日（2028/10/26）

本國民身分證晶片資料清單由柳○○自行列印

檢查碼：EL0911241916566500012OS212308904TVee97ee5F

※可至內政部戶政司全球資訊網（http://www.risgov.tw）查驗是否有效。

圖 11：國民身分證晶片資料清單(示意圖)

5. 提醒申請人，先至內政部指定網站變更用戶代碼及設定加密區、自然人憑證區密碼，說明如下：

(1) 領證確認書上載有預設之用戶代碼,請重新設定為英數字 6-10 位數字，用戶代碼須重新設定後才能用以設定加密區及自然人憑證區密碼。

(2) 請使用重新設定後之用戶代碼設定加密區密碼（PIN1，自訂密碼 6 位數字碼）。

(3) 如 New eID 有申請附加自然人憑證，請使用重新設定後之用戶代碼設定自然人憑證密碼（PIN2，自訂密碼 8-12 位數字碼）

未設定加密區及自然人憑證區密碼，未來將無法讀取/使用加密區及自然人憑證區。

6. 如申請人須諮詢 New eID 相關事項或須協助，如辦理用戶代碼變更、加密區密碼設定或變更、自然人憑證密碼設定或變更及自然人憑證之停用或廢止等，可至戶政事務所規劃之 New eID 諮詢櫃檯辦理，亦可自行於內政部指定之網站辦理。

領取 New eID 作業流程如下表所示：

表 14：New eID 領取作業

領證時間	申請人接獲戶政事務所通知領證，依所排定領證日期至戶政事務所或排定地點領取新證。
領證之戶政事務所	1. 網路申請者，向申請時指定領證之戶政事務所領取。 2. 其他申請方式，向受理申請換證之戶政事務所領取。
領證人	1. 本人領取（14 歲以上），不可委託。 2. 未滿 14 歲者，由法定代理人或由法定代理人委託當事人直系血親尊親屬陪同代為領證，本人須到場核對人貌。

應備文件	1. 舊證(初領者檢附當事人戶口名簿或身分證明文件)。 2. 印章（可簽名） 3. 領證時，舊證遺失，應檢附戶口名簿或身分證明文件及規費。 4. 法定代理人代為領證時，須另檢附其國民身分證或身分證明文件、印章（可簽名）。 5. 法定代理人之一方無法同時到時，須檢具他方領證同意書或領證委託書。 6. 法定代理人委託當事人直系血親尊親屬陪同代為領證時，須另檢附領證委託書，受託人須檢附其國民身分證或身分證明文件、印章（可簽名）。

三、銷毀作業

(一) 瑕疵卡（戶所發現品質不佳之 New eID）

New eID 為製卡中心統一製證，戶政事務所於收訖卡片進行品管時，如認定為瑕疵卡，應送回製卡中心瞭解瑕疵原因據以改進，並由製卡中心免費重新製證，逕由製卡中心進行後續銷毀作業，製卡中心並將銷毀情形報內政部備查。

(二) 非瑕疵之作廢卡（收回作廢之 New eID）

現行國民身分證由戶政事務所送所屬直轄市、縣(市）政府銷毀，尚無窒礙難行，且由直轄市、縣（市）政府集中銷毀可減輕各戶政事務所辦理銷毀人力成本外，並可防止弊端發生，爰非瑕疵卡之作廢 New eID，由戶政事務所列冊函送直轄市、縣（市）政府彙整集中銷毀，於銷毀前應專人集中保管，並將銷毀情形報內政部備查。

四、統計作業

戶政事務所人員每日下班前應執行列印「___年全面換發國民身分證統計表」，並通報直轄市、縣（市）政

府及內政部。辦理全面換證件數，不列入戶籍登記案件月統計表。

肆、數位身分識別證（New eID）例行作業

（※以下僅為初步規劃，實際情形須再與各直轄市、縣（市）政府研議協商後始得確認）

一、例行作業內容

(一) 初領：初次申請 New eID 之民眾。

(二) 補領：係指已請領 New eID，嗣後因遺失 New eID 須補領 New eID 者。

(三) 換領：係指已請領 New eID 者，嗣後因戶籍登記致 New eID 卡面記載事項變更、變更相片、New eID 毀損、重新申請 New eID 附加自然人憑證或應換領日期屆至者，須換領 New eID。

(四) 核發臨時證明書：初、補、換領 New eID 時，因無法於申辦日當日現場領取，為因應民眾緊急用證之需，得申請核發臨時證明書，作為暫時身分證明之用。

二、New eID 初、補、換領作業流程、掛失流程及晶片內容更新

(一) New eID 初、補、換領作業流程

年滿 14 歲者，以本人為申請人，未滿 14 歲者，以法定代理人為申請人。

1. 初領或補領：

本人(或法定代理人)親自向任一戶政事務所申請初領或補領；於申請時經戶政人員確認身分及資料正確後，申請人於數位簽名板上簽名，如有使用身分證明文件需求，則由戶政人員核發臨時證明書，交予申請人。

New eID 製作完畢，經戶政人員以電子郵件、簡訊或郵寄領證通知單方式通知領證後，本人前往申請之戶政事務所領取 New eID。當事人為未成年人，由法定代理人陪同當事人，前往申請之戶政事務所領取 New eID，法定代理人之一方無法陪同領取時，應出具同意書或委託書，由另一方代為領取，法定代理人亦得委託當事人直系血親尊親屬(如祖父母)為之。

領證時，請申請人檢查 New eID 外觀及確認領證確認書內容無誤後，於存根聯簽名或蓋章，New eID 及領證確認書(收執聯)由申請人攜回。

提醒申請人，部分公私立機關若尚未完成系統修正，致無法讀取晶片資料，或申請人不願需用機關(構)使用晶片讀取其個人資料者，可向戶政事務所或自行上網申請國民身分證晶片資料清單，搭配 New eID 作為身分證明文件。惟 New eID 掛失後，其國民身分證晶片資料清單暫時停止效力。

國民身分證晶片資料清單上有驗證序號，使用機關可自內政部戶政司全球資訊網（https：//www.ris.gov.tw）查驗是否有效。

(1) 申請時應備文件：

A. 本人戶口名簿或身分證明文件。

B. 法定代理人申請時，應檢附法定代理人之國民身分證或身分證明文件（法定代理人之一方無法同時到場時，須檢具其同意書或委託書）

C. 相片。

(2) 領取時應備文件及注意事項：

A. 初領：當事人戶口名簿或身分證明文件。補領:當事人戶口名簿或身分證明文件並繳交補領規費。如有領取臨時證明書者，應一併繳回。

B. 法定代理人陪同領證時，應檢附法定代理人之國民身分證或身分證明文件（法定代理人之一方無法同時到場時，須檢具其同意書或委託書）。

2. 換領：

因戶籍登記致身分證卡面記載事項變更、變更相片、New eID 毀損、重新申請 New eID 附加自然人憑證或 New eID 應換領日期屆至時，應申請換證。

於申請時經戶政人員確認身分及資料正確後，申請人於數位簽名板上簽名，因戶籍登記致身分證卡面記載事項變更應於申請換證時繳回原國民身分證，如有使用身分證明文件需求，則由戶政人員核發臨時證明書，交予申請人。因變更相片、New eID 毀損、重新申請 New eID 附加自然人憑證或 New eID 應換領日期屆至申請換證者，於領證時繳回原國民身分證。

New eID 製作完畢，經戶政人員以電子郵件、簡訊或郵寄領證通知單方式通知領證後，本人前往申請之戶政事務所領取 New eID。當事人為未成年人，由法定代理人陪同當事人，前往申請之戶政事務所領取 New eID，法定代理人之一方無法陪同領取時，應出具同意書或委託書，由另一方代為領取，法定代理人亦得委託當事人直系血親尊親屬（如祖父母）為之。

領證時，請申請人檢查 New eID 外觀及確認領證確認書內容無誤後，於存根聯簽名或蓋章，New eID 及領證確認書(收執聯)由申請人攜回。

提醒申請人，部分公私立機關若尚未完成系統修正，致無法讀取晶片資料，或申請人不願需用機關（構）使用晶片讀取其個人資料者，可向戶政事務所或自行上網申請國民身分證晶片資料清單，搭配 New eID 作為身分證明文件。惟 New eID 掛失後，其國民身分證晶片資料清單暫時停止效力。

國民身分證晶片資料清單上有驗證序號，使用機關可自內政部戶政司全球資訊網（https：//www.ris.gov.tw）查驗是否有效。

(1) 申請時應備文件：

A. 本人國民身分證。

B. 法定代理人申請時，應檢附法定代理人之國民身分證或身分證明文件（法定代理人之一方無法同時到時，須檢具其同意書或委託書）。

C. 委託他人辦理時，應檢具委託書、受託人國民身分

證或身分證明文件。

D. 相片。

(2) 領取時應備文件及注意事項：

A. 戶口名簿或身分證明文件；如有領取臨時證明書者，應一併繳回。

B. 法定代理人陪同領證時，應檢附法定代理人之國民身分證或身分證明文件（法定代理人之一方無法同時到場時，須檢具其同意書或委託書）。

3. 到府服務(由各縣市視其人力調配及資源情況決定提供服務之時機)

(1) 申請條件：有下列特殊情形經受理申請之戶政事務所認有必要者，戶政事務所派員至申請人指定地點受理申請及發證。

A. 身心障礙者。

B. 65 歲以上行動不便者。

C. 重大傷病住院或在家療養不便外出者。

D. 其他行動不便者。

(2) 申請及領取應備文件及注意事項：同臨櫃申請。

4. 戶政事務所辦理 New eID 之點收、品管檢驗新證、核發作業流程，同全面換證作業。

(二) 掛失流程及效力

民眾於遺失 New eID 時應辦理 New eID 掛失，國民身分證於掛失完成後，暫時停止其效力，自然人憑證將一

併停用。另考量國民身分證晶片資料清單係附隨國民身分證併同使用，爰國民身分證掛失時，國民身分證晶片資料清單亦暫時停止其效力。

在民眾尚未向戶政事務所提出補領前尋獲 New eID 者，可辦理撤銷掛失，撤銷掛失後自然人憑證、國民身分證晶片資料清單，一併復用。

辦理掛失之方式如下說明：

1. 臨櫃掛失身分證

本人於上班時間親自向任一戶政事務所辦理掛失。

2. 網路掛失

於內政部戶政司全球資訊網（https：//www.ris.gov.tw）辦理掛失。

3. 電話掛失

(1) 上班時間：須由本人親自撥打電話向任一戶政事務所申請辦理，但年滿 14 歲至未滿 20 歲之未成年人亦得由法定代理人代為撥打電話辦理。未滿 14 歲之未成年人由法定代理人代為辦理。

(2) 非上班時間：撥打「1996 內政服務專線」進行掛失。

4. 撤銷掛失

民眾掛失身分證後尚未向戶政事務所提出申請補領前，又尋獲身分證，得申請撤銷掛失，可臨櫃、電話撤銷掛失或上網撤銷掛失。

(三) 晶片內容更新

辦理戶籍登記、行政區域調整、門牌整編或縣(市)改制、役別變更等情形，如僅國民身分證晶片記載事項變更，卡面資料未變更，毋庸更換新 New eID，但應更新晶片內容，作法如下：

1. 申請更新國民身分證晶片資料方式

由本人（未滿 14 歲者由法定代理人）向戶政事務所辦理，本項作業得委託辦理。

2. 更新國民身分證晶片資料應備文件

(1) 本人國民身分證。

(2) 法定代理人申請時，應檢附法定代理人之國民身分證或身分證明文件（法定代理人之一方無法同時到場時，須檢具其同意書或委託書）。

(3) 委託他人辦理者，應檢具委託書、受託人之國民身分證、印章（或簽名），但因行政區域調整、門牌整編或縣(市)改制，由戶長或戶內人口代為辦理時，無須書面委託。

3. 因行政區域調整、門牌整編或縣(市)改制須更新國民身分證晶片資料，戶政事務所得攜帶行動化載具及讀卡機至指定時間及地點，於查驗申請人應備文件後，利用行動化載具進行晶片資料更新。

三、New eID 之應換領日期

(一) New eID 卡片應換領日期（年齡之計算，以申請日為基準點）：

1. 未滿 14 歲請領者：5 年。

2. 14 歲以上未滿 65 歲換領者：10 年。

3. 65 歲以上換領者：無應換領日期。

(二) 自然人憑證效期：

1. 未滿 14 歲請領者：5 年。

2. 未滿 65 歲換領者：5 年，憑證屆期可進行憑證重新簽發作業 1 次。

3. 65 歲以上民眾：其憑證在重新簽發 1 次且到期後，若用戶仍有簽發憑證之需求時，則必須換發新 New eID 卡片，或另申請憑證。

四、安全管制程序

(一) 資料審核

1. 戶政事務所應切實審核本人資料、歷次數位相片影像資料及其他附註資料，如發現資料有異，應立即透過系統回報並更新資料。

2. 受監護宣告者，不得申請自然人憑證。

(二) New eID 之作廢及銷毀程序

1. 作廢程序

(1) 適用情況：

A. 戶政事務所發現 New eID 版面或晶片有瑕疵。

B. 民眾換領 New eID，戶政事務所收回舊 New eID。

C. 戶政事務所品管檢驗 New eID 時，系統檢核民眾

有出境戶籍遷出、死亡、受死亡宣告、廢止、撤銷戶籍登記等情形，應予作廢。

(2) 戶政事務所應就收回之 New eID 以打洞機於晶片中心予以打洞，並在證卡透明視窗對角線截角作廢。

(3) 系統登錄：戶政事務所將收回之 New eID 打洞作廢後，應於系統登錄作廢情形。

(4) 集中保管作廢之 New eID：戶政事務所將作廢之 New eID 集中保管並列冊登錄於 New eID 管理系統，定期集中點交予直轄市、縣（市）政府。

2. 銷毀程序

作廢New eID之銷毀程序同全面換證期間方式，瑕疵卡片由戶政事務所列冊函送製卡中心查明瑕疵原因及銷毀，並將銷毀情形報內政部備查。

其他非瑕疵卡片之作廢 New eID 由戶政事務所列冊函送直轄市、縣（市）政府彙整集中銷毀，並將銷毀情形報內政部備查。

第拾貳章、整體架構資訊安全相關規劃

壹、 前言

依據資通安全管理法及資通安全責任等級分級辦法資通安全責任等級 A 級之公務機關應辦事項規定，辦理資安防護事宜，規劃對外 5 層、內部 4 層及委外廠商 4 層防護作業其內容為：

一、對外 5 層防護作業：布設防火牆（FW）、入侵偵測系統（IDS）、入侵防禦系統（IPS）、網路應用程式防火牆（WAF）及資訊安全監控中心（SOC），以防來自網際網路惡意攻擊之可能。

二、內部 4 層防護作業：安裝資訊資產管理及防毒軟體，辦理日誌紀錄管理及資安內部稽核，以降低內部遭受惡意攻擊或病毒感染。

三、委外廠商 4 層防護：辦理廠商權限管控、維運連線側錄、日誌紀錄管理及資安外部稽核作業，以強化廠商監督與稽核管理。

四、對資訊系統定期辦理網站弱點掃描、滲透測試及資安健診等安全性檢測，以儘早發現系統脆弱點。

貳、 共通規範

一、依照資通安全管理法及其子法、「資通安全事件通報及應變辦法」及本部「資通安全與個資事件通報及應變管理程序」規範，明確訂定各單位及委外供應商資安事件通報及應變流程與時限。

二、遵循內政部資訊系統委外服務案資訊安全管理規範（參考附錄一），並要求廠商應遵循與配合下列面向之要求

(一) 存取控制要求。

(二) 運作安全要求。

(三) 通訊安全要求。

(四) 密碼措施安全要求。

(五) 系統取得、開發及維護安全要求。

(六) 供應商關係安全要求。

(七) 資訊安全事故管理安全要求。

三、依「系統安全需求項目查檢表」（參考附錄二）作下列分類的相關檢查項目

(一) 機密性。

(二) 完整性。

(三) 可用性。

(四) 身分驗證。

(五) 授權與存取控制。

(六) 日誌紀錄。

(七) 會談（Session）管理。

(八) 錯誤及例外管理。

(九) 組態管理。

參、策略面

一、新一代國民身分證換發計畫包含規劃階段、建置階段、試行階段、全面換發階段等。於 108 年 2 月 13 日擴大成

立換發工作小組，並遴聘相關機關（單位）代表及學者專家擔任之。又規劃階段已盤點相關法規及作業辦法需修訂事項，並於 109 年 3 月 19 日發布「國民身分證全面換發辦法」。

二、在建置階段遴選資安防護良好、有豐富個資管理經驗、具有晶片卡相關技術的廠商參與，並要求廠商具有國內研發能量及在地客製化能力。此外，透過獨立驗證團隊(IV&V)及第三方資安查核團隊，監督所有的建置作業均符合工作小組指示及 ISMS/PIMS 的安全標準規範（如 ISO27001、ISO27701、BS10012 等）。上線前再邀集各界專家學者共同討論相關安全防護及配套作為。

三、規劃擇定部分縣市採民眾自願申請之方式進行小規模試辦，並辦理賞金獵人活動，開放民間團體進行黑箱測試，再全面啟動換證作業。

(一) 於試行階段蒐集民眾對 New eID 的回饋意見，並依據相關安全準則開放原始碼或開放服務，讓各界共同檢視相關設計的安全性並進行修正。

(二) 於試行階段完成所有的規範修訂，再進行全面換發。

四、全面換發階段應依據相關規範進行換發，並定期安排外部稽核以確保相關規範正確執行。各電子化政府應用導入機關也須依據規範使用 New eID，以維護資訊安全。

五、依照我國個人資料保護法第 28 條規定，公務機關違反個人資料保護法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。以每人每一事件新臺幣五百元以上二萬元以下計算。合計最高

總額以新臺幣二億元為限。故務必確保對個人資料之蒐集、處理及利用皆遵循個人資料保護法及施行細則之相關規定。

六、依照戶籍法第 75 條規定，意圖供冒用身分使用，而偽造、變造國民身分證，足以生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科新臺幣五十萬元以下罰金。行使前項偽造、變造之國民身分證者，亦同。將國民身分證交付他人，以供冒名使用，或冒用身分而使用他人交付或遺失之國民身分證，足以生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科新臺幣三十萬元以下罰金。

七、須依照資通安全管理法及其子法、「資通安全事件通報及應變辦法」及本部「資通安全與個資事件通報及應變管理程序」規範，明確訂定各單位及委外供應商資安事件通報及應變流程與時限。

八、New eID 系統由本部自行招標建置，將依政府採購法規定過濾投標廠商資格，不允許大陸地區廠商、第三地區含陸資成分廠商及在臺陸資廠商參與，另 New eID 相關系統將建置於內政資料中心之內網環境，該中心可提供「共用雲端基礎服務」優質基礎設施與網路資安環境，完善整體資訊安全防護，並符合資通安全管理法規範及資安防護達到 A 級之公務機關應辦事項，完善資通安全。

九、本部將訂定申請及稽核規範，據此規範審核需用機關（構）申請讀取加密區特定欄位之必要性及讀取期限，且需用機關應接受本部稽核，確保資料使用安全。

肆、管理面

一、安全管理措施

(一) 設備安全:委外廠商人員所須存取之資料或攜入之資訊設備，包括個人電腦、平板電腦、行動電話、智慧卡及所有形式的儲存設備等,於機關場所內使用任何資訊處理設備均應受管理。

(二) 門禁管理:委外作業人員進出工作場所，均應配帶員工證件，非經許可不得至工作場所以外地區活動，且須由本機關人員陪同作業。

(三) 供應鏈管理：

1. 資訊委外廠商人員需簽署保密切結文件，人員資格須經過審核才可擔任（參考附錄三）。

2. 資通安全機制監督與稽核(含帳號權限審核紀錄、存取紀錄資料之稽核）。

3. 特殊機敏資料存取授權（含職責分工(separation of duty)、多人控管(dual control)、限制行動化裝置使用、對外網路連線過濾等）。

4. 晶片卡片：

(1) 卡片提供廠商需佐證相關製作流程具有備援機制，確保主/備援晶片均能滿足功能需求，且具有長期供應的能力，定期召開安全檢視會議，以評估各晶片是否安全或需要更換。

(2) New eID 之 COS(IC 卡作業系統,Chip Operating System)與 applet(小程式)均須通過 CC 國際驗證(安全評估共通準則, Common Criteria），並提供給晶

圓廠於生產階段即燒入晶片，讓晶片更安全。

5. 資訊系統：於可控之安全場地進行開發環境測試與建置，包含整合式開發環境（IDE）、軟體開發套件（SDK）等。

二、New eID 於中央印製廠嚴格管制的安全製發場地集中製卡，系統採封閉式作業，資料以專線加密傳輸，空白晶片卡運送時採取加密保護措施，防止未經授權之存取，運達中央印製廠後，進行晶片卡控制權移轉(俗稱洗卡作業)，驗證卡片安全狀況。並由本部監督中央印製廠專責人員進行印製工作，又該廠人員為國營事業員工，受相關法規之拘束，整體製程均有層層安全管控、專人保全運送至戶政單位，以保障民眾個人資料安全。

三、New eID 將卡面個資最小化，只保留姓名、國民身分證統一編號、出生日期、相片及結婚狀態。其餘個人資料如戶籍地址、父母姓名則保存在晶片內，須輸入讀取碼或密碼才能讀取。

四、使用 New eID 不會在內政部留下使用紀錄，民眾辦理任何服務，相關紀錄均留存於各服務提供機關，須依個人資料保護法妥善管理，並防範資安事件發生，避免資料竊錄或個資外洩情形，以保障民眾隱私。

五、New eID 系統建置規劃同地及異地備援機制，確保風險發生時服務不中斷。

六、建置「授權驗證系統」，控管需用機關讀取 New eID 之加密區資料，需用機關除須取得民眾同意且須輸入密碼（PIN1）外，尚須取得本部審查授權需用機關依其執行

法定業務所需後簽發之憑證，始得以 Secure API 讀取加密區資料，以保護民眾相關隱私。

七、研議需用機關開發應用系統應遵循之應用系統使用 New eID 之安全檢查表（暫定），供需用機關作為系統安全檢查之依據。

八、依照「資通安全管理法」及其子法、「資通安全責任等級分級辦法」以及本部「委外供應商關係管理程序」，確實執行委外供應商管理，包括：委外供應商資通安全政策訂定、資通訊技術供應鏈管理、委外供應商服務監視與審查、服務變更管理等，以落實委外供應商管理。

伍、技術面

一、應用程式開發應遵循安全系統發展生命週期（SSDLC），於系統開發各階段納入安全評估與安全措施，確保系統安全。

二、應於封閉網路進行應用程式開發、維運及管理作業。

三、應用系統、資料庫及網域主機密碼應符合長度與複雜度原則，且勿使用弱密碼及鍵盤順序。

四、開發環境其程式原始碼之存取權限應予控管（含版本控制、源碼檢測、佈署管理等）。

五、系統設計應採取個資最小化原則。

六、建立資安弱點通報機制，得以即時辨識系統軟硬體之資安弱點。

七、應用程式上線前或功能變更時，須進行相關風險評估與技術檢測（源碼檢測、弱點掃描）。

八、將系統建置於內政資料中心之內網環境中，對外連線系統採用虛擬專用網路（VPN），並設有防火牆入侵偵測

及防護機制，確保資料通訊安全。

九、依據「內政部憑證管理中心憑證作業基準」規範，晶片金鑰對須於晶片中自行運算產生，確保私密金鑰無法匯出、重製。

陸、 維運面

一、完善的權限控管機制。

二、異常行為監控及紀錄

依據「政府機關（構）資通安全責任等級分級辦法 A 級之公務機關應辦事項」規定辦理下列事宜：

(一) 針對資訊系統定期辦理網站弱點掃描、滲透測試及資安健診等安全性檢測；資安責任等級「高」之資訊系統須辦理源碼檢測事宜。

(二) 建立資安防禦縱深，部署 IDS/IPS、WAF 應用程式防火牆、郵件過濾裝置、防毒軟體及進階持續性威脅攻擊防禦措施等資通安全防護事宜。

(三) 應針對正式區域伺服器、各式主機佈署應用程式白名單機制，並檢驗確認可僅允許經過授權之程式執行，阻擋不在白名單之內的應用程式，並且當未經授權程式嘗試執行時通報資安監控中心或是其他中控管理系統。

(四) 建立資訊安全監控中心(SOC)，執行 7*24 小時惡意活動偵測、監控及通報，即時掌握網路威脅，快速回應資安事件。

(五) 辦理資通安全教育訓練，提升同仁資安防護意識，提高資安警覺性。

三、定期檢視作業系統日誌及網站日誌，並依資通安全管理法及本部資訊安全管理制度(ISMS)規定辦理日誌之管理與保存作業。

四、針對作業系統、系統開發元件應定期檢視是否存在資安漏洞並進行修補事宜。

五、政府組態基準(GCB)：依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。

六、定期的內外部資安稽核

(一) 依據「政府機關（構）資訊安全責任等級分級作業施行計畫」規範中定義，除希望政府機關能遵守行政院及所屬各機關資訊安全管理規範外，各機關應依其不同資安等級規劃稽核方式如下：

1. A 級單位每年至少執行 2 次內部稽核。

2. B 級單位每年至少執行 1 次內部稽核。

3. C 與 D 級單位得執行自我檢視。

(二) 內外部資安稽核

表 15：資安稽核項目表

資安稽核	項目
內部資安稽核	針對業務應用系統、應用程式（含 API 及 APP）與資料庫保留詳細操作紀錄並提供資安稽核機制。
	針對系統帳號之行為進行記錄，並進行分析，確保無高風險之操作行為，並通知系統管理者。
	系統針對系統管理者及使用者之操作行為進行紀錄，並根據頻率及規則分析，確保無高風險之操作行為。

	應用程式（含 API 及 APP）與資料庫應能針對使用者之操作行為進行記錄，可與登入應用程式帳號關聯，並根據數值、命令、時間、地點、頻率等行為訂立規則分析，確保無高風險之操作行為。
外部資安稽核	業務應用系統應記錄使用者之登入與登出之行為，分析出異常行為並通知該帳號擁有者。
	業務應用系統應記錄使用者登入失敗之行為，分析出異常行為並通知管理者與該帳號擁有者。
	業務應用系統應紀錄系統事件並分析異常使用行為。

柒、採購面

依政府採購法規定過濾各階段的投標及參與廠商資格，不允許大陸地區廠商、第三地區含陸資成分廠商及在臺陸資廠商參與。

另基於製卡涉及場域安全、卡片防偽、秘密諮詢、專屬權利等考量，且國外先進國家如德、法等國亦基於安全考量委由國家級印製廠辦理卡片印製工作，爰依政府採購法第 22 條第 1 項第 2 款規定，採限制性招標委由國家級的中央印製廠辦理 New eID 印製作業。

捌、執行面

一、資安風險分析

針對相關系統（製卡中心端、系統端、卡片端）可能產生之資安風險威脅進行分析，列舉如下表：

表 16：資安風險威脅分析

	製卡中心端	系統端	卡片端
風險威脅	使用者的不當操作	非法人士攻擊入侵或當作攻擊跳板	空白卡及成卡不當保存
	非上班時間於廠內活動	惡意的軟體下載及操作	晶片遭入侵攻擊
	異常的資料接收印製	APT 郵件攻擊	加密演算法被破解
	資訊安全意識及訓練不足	使用者不當操作	使用者密碼被破
	存取管制政策不完善	存取管制政策不完善	存取管制政策不完善
	未適當管理於組織外部工作的員工	網頁竄改	晶片資料遭竄改
	作業人員對個人資料保護考慮不完善	不適當的網路管理	卡體破壞
	通訊線路交接處理不佳	授權失效	晶片內資料被竊
	機密/敏感資訊竊取或破壞	病毒感染破壞	隱私資料洩漏
	未定期檢視視訊監控錄影系統	個人隱私資料不當公開	空白卡及成卡的運送安全
	不適當的網路管理	竄改或刪除資料庫資料	
	軟體的下載與使用未管制	硬體損壞	
	惡意的軟體下載及操作		
	竄改或刪除資料庫資料		

以上資安風險威脅相關因應措施，依據資安事件處理機制及資訊安全共通規範進行管理，分述如後。

二、資安事件處理機制

(一) 事前準備

1. 成立資安監控中心

(1) 資安監控中心執掌如下：

圖 12：資安監控中心執掌

(2) 監控小組分工如下：

表 17：監控小組分工

組織名稱	成員	工作職掌
資安監控中心	• 技術總監 • 專案經理 • SOC 平台 • 事件監控維運小組 • 緊急應變處理小組 • 教育訓練小組	• 審核並頒行資安監控程序 • 定期檢討資安監控成效 • 定期提交資安防護執行報告 • 定期提交資通安全整體評估報告 • 維持資安監控正常運作 • 配合資安政策履行監控策略
SOC 平台組	• 系統維運人員 • 系統開發人員	• 負責資安監控平台規劃建置、開發與維運 • 負責應用程式系統管理
監控維運小組	• 一線值班安全工程師 • 二線資安技術工程師 • 資安事故管理小組	• 日常事件監控、通報、追蹤、分析及處理 • 定期撰寫資安防護執行報告
緊急應變處理小組	• 事故發生單位人員 • 鑑識人員 • 二線資安技術分析師 • 資安事件管理小組	• 緊急事故鑑識 • 提交鑑識報告
教育訓練小組	• 內部講師 • 外聘專家 • 資安事件管理小組	• 協助宣導資安政策等相關規定 • 定期辦理資安新趨勢及技術講座 • 培訓資安人員

(3) 資安監控中心分工

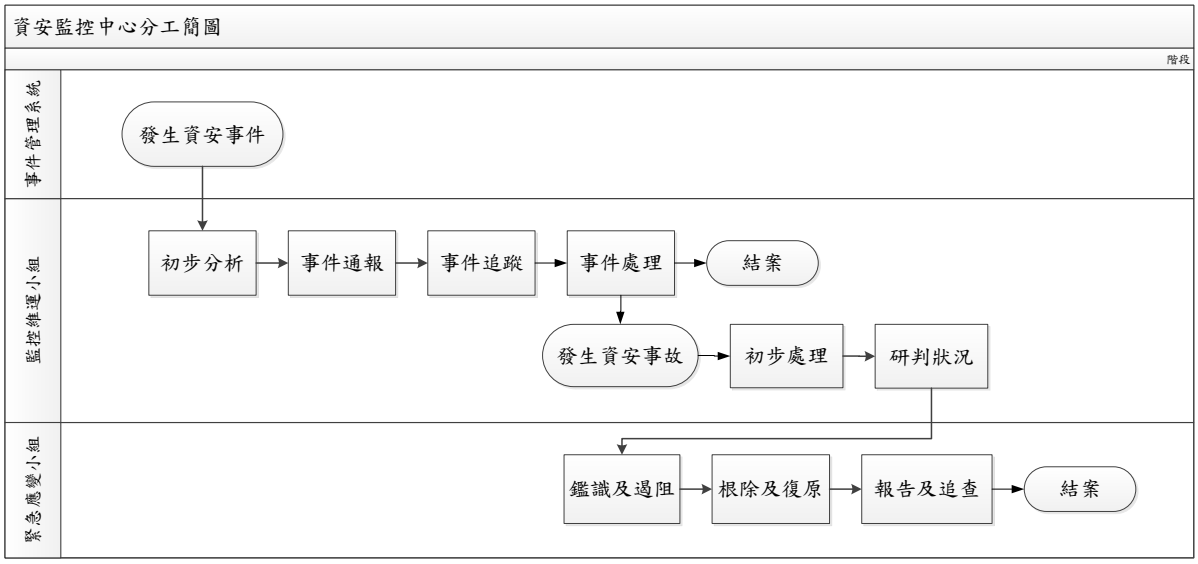


圖 13：監控小組分工

(4) 資料庫、應用程式、APP 及資安設備之日誌並進行關聯分析。

(5) 建立資安監控程式

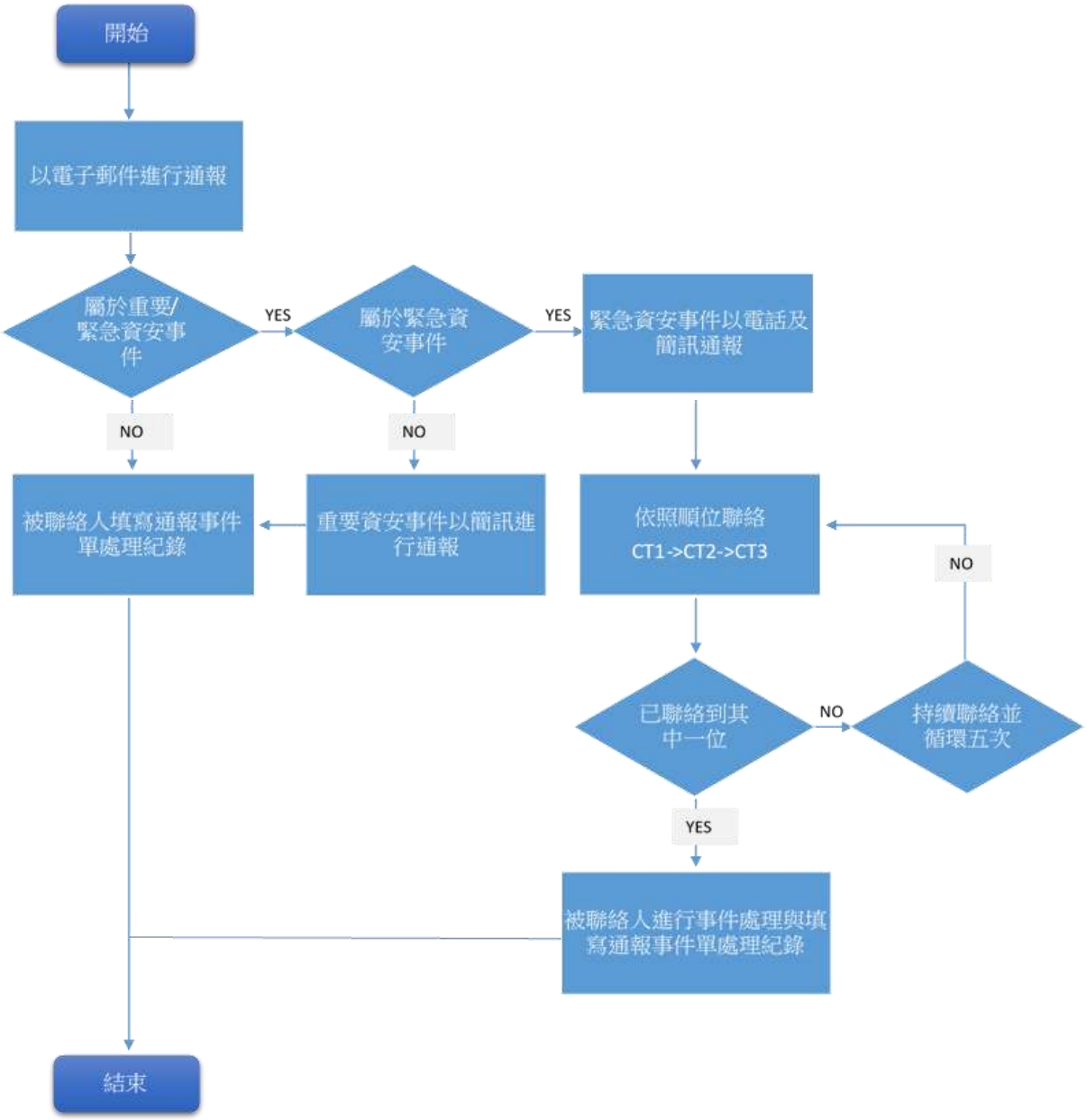


圖 14：資安事件電話及簡訊通報程序

(二) 事中因應

1. 當事故發生時，經一線人員研判分析其事件之嚴重等級，依下列通報方式及通報對象進行通報。通報層級分為一般資安事件、重要資安事件及緊急資安事件 3 種，詳如下表。

表 18：通報方式

通報層級	分類	通報方式
一般資安事件	低風險事件	電子郵件
重要資安事件	中風險事件	5×8電話 電子郵件 簡訊
緊急資安事件	高風險事件	7×24電話 電子郵件 簡訊

2. 資安事件通報對象如下：

表 19：通報對象

1. 資安聯絡窗口：

(1)第一順位（CT1）

(2)第二順位（CT2）

(3)第三順位（CT3）

1. SOC中心：

(1)SOC中心二線（CM1）

(2)SOC資安主管（CM2）

通報層級	分類	電子郵件通報對象
一般資安事件	低風險事件	資安聯絡窗口（CT1） SOC中心二線（CM1）
重要資安事件	中風險事件	資安聯絡窗口（CT1、CT2） SOC中心二線（CM1）
緊急資安事件	高風險事件	資安聯絡窗口（CT1、CT2、CT3） SOC中心二線及資安主管（CM1、CM2）

(三) 事後處理

資安事件鑑識及分析，找出事件根因並進行改善：

1. 通知該業務資安聯絡人及業務負責人，保存相關系統證據以進行後續資安鑑識，保存方式須依照證物鏈方式進行保存。

2. 針對系統、應用程式及資安設備日誌進行分析，應包含登入登出、事件、系統功能操作、資安設備告警等日誌進行分析。

3. 提出鑑識結果報告與後續改善說明。

(四) 資料庫備份：

1. 定期完整備份：系統設定每週六晚上進行完整備份作業，自動將資料庫完整備份（含資料檔與參數檔）至指定磁碟路徑。

2. 每日差異備份：系統設定每日晚上 24：00 進行當日差異備份，將當日日誌紀錄檔，自動備份至指定磁碟路徑。

3. 外部備份：依據設定作業，每日自動進行外部磁帶備份作業。

4. 異地備份：依據系統管理者設定，每日自動進行備份資料傳輸至其他主機，進行異地備份檔案存放作業。

(五) 系統回復處理

1. 應用程式復原：採用快速安裝程式復原作業系統，依據備份媒體操作方式回存程式與參數檔案至主機系統，依據程式所需之屬性進行相關設定。

(1) 資料檔復原：完成主機系統與程式復原後，依據最新備份資料檔進行資料庫復原作業，並依據每日差異備份檔案，進行資料檔還原作業。

(2) 資料庫重整：資料還原完成後，採用資料庫指令進行資料表重整作業，建立資料索引順序，完成系統復原作業。

(六) 系統還原

1. 備援主機即時轉換時間

接獲系統異常通知後於資通安全管理法及相關規範要求之時間內還原系統，完成系統復原或備援作業，若本案系統硬體發生故障，亦可配合於指定硬體中復原系統，持續提供相關服務：

(1) 程式及參數復原作業：60~80 分鐘。

(2) 資料庫復原作業：依資料量多寡。

(3) 資料重整復原作業：依資料量多寡。

2. 備援步驟

(1) Step 1：備援主機快速安裝系統完成。

(2) Step 2：程式復原作業。

(3) Step 3：資料庫復原作業。

(七) 應定期進行災難復原演練及業務持續計畫檢討。

三、資安及作業流程管理規則

(一) New eID 管理系統及製卡中心端資安防護規範

1. 資訊安全通則

(1) 各項資通安全解決方案,具備資安產品認證之產品為佳，如安全評估共同準則（Common Criteria）、ICSA Labs 認證、NSS Labs 認證。

(2) 系統如需透過網路傳輸，應採用 TLS1.2 含以上或專屬傳輸層通道加密設備安全通訊協定進行保護為原則。資料如經外部媒體，如 USB 隨身碟、光碟或其他外接觸存取裝置交換，應以加密格式儲存,並應限定僅特定經認證裝置或應用程式方可讀取使用。

(3) 重要應用系統及服務如發生「異常中斷」、「效能低落」、「異常交易」或「無法正常服務」等皆視為資安事件，應建立有效管理及監控機制，以及時處理異常事件，回復服務效能。

(4) 系統間應有隔離機制，依服務系統重要性，至少進行分區隔離,重要核心系統應依據該系統應用服務再設定個別化細分隔離規則。僅有允許之連線可以通過，避免惡意程式感染擴散之狀況。

(5) 戶所端應比照內政部實體隔離環境使用管理要點進行資安管理作業,針對戶所進行遠端更新所使用主機進行實體隔離作業,並指定同仁擔任管理實體隔離環境所配置之個人電腦及週邊設備之負責安全防護工作，以防範機密資料外洩。

(6) 應設置系統、網路、應用程式及資安監控中心（Security Operation Center，SOC），針對系統、網路、應用程式可用度及資安事件進行監控通報處理。

(7) 針對系統服務對資料提取與運用，應確實留下不可抹除之日誌紀錄，以作為資料正當使用之操作稽核。

(8) 各區域之主機及設備日誌應整合至資安監控中心進行監控分析。

(9) 遭受資安攻擊事件時，應立即聯繫轄屬廠商以及進行資安事件通報，並視事件影響範圍關閉相關服務。

(10) 確認資安事件修復後啟動相關還原機制，以回復系統服務正常運作。

(11) 完成服務還原後視資安事件嚴重層級與相關單位進行後續檢討作為，提報資安事件發生流程與相關日誌紀錄檔，確認資安事件發生原因以及攻擊路徑，以確保相關資安解決方案與事件處理流程符合預期目標。

(12) 若相關事件處理流程需要調整，則提出後續改善機制，以滾動式修正完備資安事件因應作為。

(13) New eID 管理系統或製卡中心端或管理規則之適用對象，分別依據業務性質遵循管理規則之作業要求。

2. 資訊安全管理

(1) 資訊安全管理系統之導入及通過公正協力廠商之驗證，於 1 年內全部核心資通系統導入 ISO 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於 2 年內完成全系統公正協力廠商驗證，並持續維持其驗證有效性。

(2) 配置資通安全專責人員，且須以專職人員配置。

(3) 每年辦理 2 次內部資通安全稽核。

(4) 全部核心資通系統每年辦理 1 次業務持續運作演練。

(5) 每年辦理 1 次資安治理成熟度評估。

(6) 存取控制規範：

A. 所有作業均需專人負責，並依照職務給予不同之帳號權限控管，人員不得進入未經授權之系統，所有系統必須記錄帳戶之登入紀錄、登入後執行之所有工作內容及登出紀錄，另系統應具有身分識別管理機制，每季提供安全機房人員進出管制紀錄。

B. 帳號管理：逾越機關規劃預期閒置時間或可使用時間，系統應自動將使用者登出；應監控系統帳號以及異常使用並回報管理者、建立帳號管理機制，包含定期檢視系統帳號是否逾期、閒置，審核帳號之建立、修改、啟用、禁用及刪除。

(7) 系統具有稽核功能以及可歸責性：定期審查稽核事件，系統有稽核特定事件之功能，並保留稽核紀錄（含稽核失效之回應、稽核紀錄應具有時戳與校時、保護稽核紀錄），稽核紀錄應包含事件類型、發生時間、發生位置以及事件相關使用者身分識別等資訊。

(8) 系統應採用加密機制，以保障傳輸之機密性與完整性與資料儲存之安全。

3.安全性檢測

(1) 所開發之應用程式（含 API 及 APP）上線或改版前，應進行「源碼掃描」安全檢測，源碼掃描包含源碼及第 3 方程式庫檢測，確保無中等級風險以上或是造成機敏資料外洩之漏洞，以保障系統安全。

(2) 上線之應用程式 App（含 iOS 及 Android 版本）應通過經濟部工業局規範之行動應用 App 基本資安檢測基準，針對「行動應用程式發布安全」、「敏感性資料保護」、「行動應用程式使用者身分識別、授權與連線管理安全」、「行動應用程式碼安全」等項目進行測試，且核符第 2 類層級：具識別功能與連網行為應用程式要求，確保無相關資安漏洞。

(3) 應於上線前針對網站服務、需用機關應用系統及 New eID 相關存取設備等進行弱點掃描與滲透測試，確保無中等級風險以上之漏洞，低等級風險漏洞應確認其風險原因，應適度進行修復動作。

(4) 應用程式、網站服務、應用系統、存取設備若檢測

出中等級風險以上漏洞時，須於資通安全管理法及相關規範規定時間內修補完畢，或是採行適當之補償性措施經認可後予以豁免，以確保其安全。

(5) 新上線之系統應於上線前針對部署系統環境進行掃毒，確認相關作業系統環境內不包含任何惡意程式及惡意活動。

(6) 相關系統、應用程式 App（含 iOS 及 Android）、設備應至少每半年執行 1 次定期安全性檢測，並且相關系統與應用程式進行版本更新時，於上線前需要執行安全性檢測。

(7) 系統及設備應至少每 3 個月進行一次密碼修改，並確認密碼長度至少涵蓋 8 個字符（建議包括 14 個字符或更長），由包括大小寫字母、數字和符號在內的組合。

4. 資通安全健診

應每年辦理 1 次資通安全健診，內容包含網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視與目錄伺服器設定及防火牆連線設定檢視。

5. 資通安全威脅偵測管理機制

(1) 1 年內，完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。

(2) 應導入業界主流之安全性資訊與事件管理系統（Security Information and Event Management, SIEM），用以整合本案之各軟硬體系統、網路系

統、安全防護系統、客製化應用程式及 API 服務群集等元件之日誌、SNMP 紀錄、檔案及事件等各種資料源，並進行彙整（Aggregation）、過濾、分析、監視及異常告警，與其他相關之處理。

(3) 應整合運用本案之相關系統工具（如次世代防火牆、端點防護軟體、網頁應用防火牆等）及資料來源（系統、應用程式、資料庫、物聯網裝置等），以實作本案之系統健康狀態及資安風險監控與警告之機制。

6. 政府組態基準

1 年內，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。

7. 資通安全防護

(1) 系統與主機應安裝防毒軟體，並確認維持病毒碼更新至最新版本。

(2) 應導入業界主流之企業網路防火牆 （Enterprise Network Firewall），並建議導入次世代防火牆，以具備 IPS/WAF/IDS/ASP 等攻擊防禦與入侵偵測機制。

(3) 系統間應有隔離機制，僅有允許之連線可以通過，避免惡意程式感染擴散之狀況。

(4) 提供 APT 進階持續性威脅攻擊防禦措施，可針對惡意郵件進行過濾，透過有效分析方式找出並阻攔惡意電子郵件攻擊。

(5) 應針對正式區域伺服器、各式主機佈署應用程式白名單機制，並檢驗確認可僅允許經過授權之程式執行，阻擋不在白名單之內的應用程式，當未經授權程式嘗試執行時通報資安監控中心或是其他中控管理系統。

8. 資通安全教育訓練

(1) 資通安全及資訊人員每年至少 4 名人員各接受 12 小時以上之資通安全專業課程訓練或資通安全職能訓練。

(2) 一般使用者及主管每人每年接受 3 小時以上之一般資通安全教育訓練。

9. 資通安全專業證照及職能訓練證書

(1) 1 年內，資通安全專職人員總計應持有 4 張以上資通安全專業證照，並持續維持證照之有效性。

(2) 1 年內，資通安全專職人員總計應持有 4 張以上資通安全職能評量證書，並持續維持證書之有效性。

10. 災害復原及業務持續機制

(1) 應對於惡意程式及勒索軟體等新式入侵攻擊及破壞手段，提出有效可行之防護及復原對策，並於本案進行實作。

(2) 前述復原對策應具備自發現惡意程式或勒索軟體入侵情形後，於資通安全管理法及相關規範要求時間內，將系統及資料回復至未受入侵或破壞前狀態之能力。

(3) 系統備份：

A. 程式與系統參數備份

(a) 常態性備份：系統安裝完成後，完整備份。

(b) 異動備份：透過版控系統或手動記錄並備份歷次更新程式版本。

(c) 快速安裝程式：透過可編輯安裝指令，建立系統環境自動安裝光碟，可於 4 小時內快速完成系統程式服務建置設定。

(二) 應用端資安防護規範

1.遠端更新資安防護規範（戶政事務所作業端）

(1) 應用程式得提供通知訂閱功能，當存取民眾 New eID 內資料時，將可透過應用程式或電子郵件等訊息推播方式使民眾掌握資料存取狀況。

(2) 戶所人員於戶所端受理民眾之 New eID 晶片資料更新時須確認民眾身分，方能進行遠端更新作業程式，整體程式須符合「不可否認性」與「可驗證性」等安全特性。

(3) 遠端更新作業程式進行前，須先檢驗該次資料異動需求是否適用於「遠端更新」。若民眾異動之資料為列印於 New eID 外觀版面之項目，則表示該次需求並不適用「遠端更新」，須告知民眾換發實體 New eID。

(4) 遠端更新作業程式必須具備點對點通道加密機制，由資料提供端至卡片端，須保障整段資料傳輸過程

皆為加密傳輸，防止資料遭受不當竊取與竄改，過程中必須能夠有效防禦中間人攻擊 （Man-in-the-middle attack）、重送攻擊 （Replay attack） 等網路攻擊行為；另外，也必須保證更新後資料確定為 New eID 後端合法核發與更新之資料，整體機制須符合「機密性」與「完整性」等安全特性。

(5) 遠端更新作業程式必須具備資料提供端、卡片端等雙方身分及授權確認機制，資料提供端必須能夠向卡片端證明自身具備晶片內容更新權限，而卡片端必須向資料提供端證明自身卡片之合法性與有效性。當雙方身分與授權完成確認後，方能進行晶片內容更新作業。

(6) New eID 後端系統架構須採用 HA （High Availability） 高可靠性系統架構提供遠端更新服務，且應有完善之稽核軌跡紀錄，整體架構須符合「可用性」與「可歸責性」等安全特性。

(7) New eID 後端系統架構上線前需根據安全性檢測規定進行上線前安全檢測，包含滲透測試與弱點掃描，如有 APP 則須配合行動裝置作業系統改版進行 APP 檢測。

(8) New eID 後端系統應針對正式區域伺服器佈署應用程式白名單機制，僅允許經過授權之程式執行。

(9) 當資安事件發生時需儘速暫停必要之 API 串連服務，並且保存當時狀況下之資料庫與日誌資料，以及事發當下所有機器狀態。

(10) 完成資安事件修復後，依據備援還原機制進行服務還原，完成應用端資安事件事中緊急應變處理。

(11) 根據事件鑑識處理判定應用端服務漏洞以及攻擊成因並召開調查會議,根據漏洞層級與災損狀況研擬系統設計流程或漏洞相關設計細節之修正可能（包含系統管理權限、防火牆規則、安全性漏洞修補等具體改善措施）。

(12) 事件鑑識處理完成後，則就事件相關聯的脆弱點擬定補強方案，並於 API 或相關應用端服務相關修補作業完成後委請協力廠商進行驗測確認。

2.API 資安防護規範

(1) 資安檢測

業務應用系統上線前需進行上線前安全檢測，上線後需每半年以及每次進行更版作業時亦須接受安全性檢測。

(2) 個資保護機制

需用機關調用加密區個資時，New eID 管理系統僅記錄需用機關之授權狀態，用以統計讀取次數並檢核該需用機關權限，不記錄被調用民眾之相關個資資訊。需用機關之業務應用系統，應留存民眾同意與使用資料之紀錄。

(3) 資安稽核紀錄

A. 應針對業務應用系統、應用程式（含 API 及 APP）與資料庫保留詳細操作紀錄並提供資安稽核機

制。

B. 業務應用系統應記錄使用者之登入與登出之行為，分析出異常行為並通知該帳號擁有者。

C. 業務應用系統應記錄使用者登入失敗之行為，分析出異常行為並通知管理者與該帳號擁有者。

D. 業務應用系統應紀錄系統事件並分析異常使用行為。

E. 應針對系統帳號之行為進行記錄，並進行分析，確保無高風險之操作行為，並通知系統管理者。

F. 系統應針對系統管理者及使用者之操作行為進行紀錄，並根據頻率及規則分析，確保無高風險之操作行為。

G. 應用程式（含 API 及 APP）與資料庫應能針對使用者之操作行為進行記錄，可與登入應用程式帳號關聯，並根據數值、命令、時間、地點、頻率等行為訂立規則分析，確保無高風險之操作行為。

3.網站

(1) 應定期進行網站弱點掃描，網站弱點掃描及滲透測試作業，須涵蓋 OWASP Top 10 等常見資安威脅。確保不論是在黑/白箱或灰箱模式皆無中等級風險以上之漏洞，當發現中等級風險以上之漏洞，應於資通安全管理法及相關規範要求時間內修補完畢或提出對應方案。

(2) 所有網站上線或大改版前，應進行網站弱點掃描，

確保不論是在黑/白箱或灰箱模式皆無中等級風險以上之漏洞，低等級風險漏洞需有合理解釋。

(3) 使用 New eID 附加自然人憑證於網路身分識別搭配公開區及加密區資料驗證時，應完成以下驗證程序：

A. 依公開憑證處理之安全檢查表驗證憑證及數位簽章。

B. 依 New eID 資料驗證安全檢查表（暫定）驗證公開區/加密區資料。

C. 確認憑證及 New eID 資料是同一人。

(三) 卡片端安全防護

1.晶片安全規範與規格

晶片作業系統、資通產品等須符合國際標準，如資訊技術安全評估共同準則(Common Criteria,CC)、ISO/IEC 15408 驗證，並取得安全評估保證等級（EAL4+）以上安全認證，接觸式須符合 ISO 7816-3，非接觸須符合 ISO 14443(須在數釐米內始可感應)。另晶片私密金鑰對產製是依據內政部憑證管理中心憑證實務作業基準（CPS）規範，金鑰對須在晶片中自行運算產生，確保私密金鑰無法匯出、重製，任何人都無法取得該私密金鑰，也無法被製卡廠商掌握私密金鑰。

2.晶片存取安全規範

(1) 讀取戶籍地區

A. 讀取戶籍地區欄位資料。

(2) 讀取公開區

A. 輸入讀取碼（CAN），驗證 CAN 讀取資料，經由基本存取控制（Supplemental Access Control），產生金鑰並驗證後建立安全通道（Secure Channel）。

B. 讀取公開區欄位資料欄位。

C. 檢驗晶片的合法性，經由主動驗證（Active Authentication，AA），驗證晶片是否為內政部核發非偽造。AA 私鑰採取 ECC P-521 演算法並存於卡片中，無法匯出。

D. 經由被動驗證（Passive Authentication，PA），驗證公開區資料是否正確。

(3) 讀取加密區

A. 讀取加密區資料，在建立安全通道(Secure Channel)的狀態下，請持卡人輸入 New eID 的 PIN1 密碼，經由密碼管理（PIN Management）機制確認是否為民眾合法授權讀取並驗證密碼。

B. 經由終端驗證（Terminal Authentication，TA）驗證讀取單位是否有無權限可以讀取內政部授權的相關欄位。

C. 檢驗晶片的合法性，經由晶片驗證（Chip Authentication，CA），驗證晶片是否為內政部核發非偽造。CA 私鑰採取 ECC P-521 演算法並存於卡片中，無法匯出。

D. 讀取授權的資料欄位。

E. 經由被動驗證（Passive Authentication，PA），驗證資料是否正確。

(4) 讀取自然人憑證區

A. 利用金鑰交換演算法建立安全通道。

B. 使用者輸入 PIN2 驗證是否正確，若連續錯誤達三次則鎖定卡片。

C. 讀取使用者的簽章或加密憑證。

D. 使用者利用私密金鑰進行簽章或解密。

E. 驗證解密結果或簽章結果。

3.卡片安全性相關規範

(1) 每張 New eID 晶片要有單一識別碼（Unique ID, UID），用於生產及履歷管理使用，避免晶片外流、盜用或不當使用，另在寫入個人化資料後，啟動晶片之隨機亂數序號，每次感應都重新產生不同的隨機亂數，無法連結個人資訊，自無法追蹤晶片使用軌跡，與目前的晶片護照作法相同。

(2) 晶片硬體需通過安全認證 Common Criteria EAL 5+（含）以上，晶片須可防範電子 SPA/DPA（Power Analysis）、Trimming、DFA（Differential Fault Analysis）等攻擊，及可承受各式物理（電壓、音波、溫度、光）衝擊。New eID 使用之作業系統及軟體(Applet)需通過安全認證 common criteria EAL 4+（含）以上。

(3) 卡廠及製卡中心應取得 ISO14298、EMV（Europay, Mastercard, and Visa）或 PCI-DSS（Payment Card Industry Data Security Standard）其一認證。

(4) 內政部保有對卡廠及製卡中心為不定期稽核作業，以確保卡廠及製卡中心確實執行 New eID 製發之作業程式。

(5) 產品庫房安全管理，應保存庫房文件紀錄、規劃卡片存放區、庫房檢核管理、卡片出入庫管制、耗材管理、廢料及廢卡控管，及控管壞卡、報廢卡。

(6) 包裝管制：

A. 卡片裝盒方式

(a) 卡廠應以 250 張或 500 張卡片為單位將卡片裝於卡盒內。

(b) 卡盒需有封裝防潮，每盒外包裝需標註盒號、生產批號、產品名稱、作業系統名稱、PC 卡數量及製造日期等資訊（可由盒號查詢前項交貨資料之晶片 ID 資訊）。

B. 卡片整批裝箱方式

(a) 卡盒應裝於堅實之箱匣內，並以適當保護材料填實，以防遞送途中，物與物或物與箱壁間之摩擦或碰撞。卡片之箱匣外應以彌封條加以彌封，以加強控管。

(b) 箱上應有識別條碼，此識別條碼之編碼應同時可為人工判讀並合於標準條碼型式。

C. 運送管制：尚未初始化作業之空白卡（含晶片）及空白卡（含晶片）經 Gen Key 作業均採全程安全運送規格。

4.卡片召回程序

如 New eID 晶片發生安全問題而需進行召回時，依下列步驟進行：

(1) 評定安全影響範圍與召回成本，確認召回層級與範圍。

(2) New eID 管理系統列出擬召回之證件，確認召回數量。

(3) 確認召回晶片卡處理方式（韌體更新或換領新證）。

(4) New eID 管理系統廢止卡片序號對應之卡片，並提供 OCSP 及 CRL 名單進行查詢。

(5) 在 New eID 專屬網站公告，並通知需用機關公開區、加密區及自然人憑證區停用 API，且不提供下載服務，同時進行 API 修改。API 修改後公告並通知需用機關，需用機關須強制更新 API 後始能繼續使用 OCSP 及 CRL 查詢服務。

(6) 以簡訊、電子郵件或電話通知民眾持舊證辦理韌體更新或申請換領新證。

(7) 戶政事務所受理民眾持舊證韌體更新或申請換發新證，如有特殊情形如身心障礙、65 歲以上行動

不便、重大傷病住院或在家療養不便外出、其他行動不便，經戶政事務所認有必要時，得派員至民眾指定地點到府受理。

(8) 戶政事務所依前項規定受理民眾申請換發時，應收回舊證打洞，並開立臨時證明書予民眾。

(9) 戶政事務所需定時回報內政部韌體更新或換證作業進度。

(10) 製證完成並運送至戶政事務所時，由該戶政事務所通知民眾領取新證，如有特殊情形如身心障礙、65 歲以上行動不便、重大傷病住院或在家療養不便外出、其他行動不便，經戶政事務所認有必要時，得派員至民眾指定地點到府受理領證作業。

(11) 保存相關召回紀錄以備日後查核之用。

玖、資通安全共通規範

為保障相關資訊系統安全及機密，應遵循之相關法令規定：

一、資通安全管理法及其子法。

二、個人資料保護法及子法。

三、行政院及所屬各機關資訊安全管理規範及要點。

四、內政部資訊系統委外服務案資訊安全管理規範。

五、內政部委外服務案個人資料保護規範。

六、內政部資訊安全暨個資保護管理制度相關規範。

七、內政部系統安全需求項目查檢表。

八、戶役政資訊系統安全管理手冊。

壹拾、 資訊安全經費

New eID 整體之資訊安全防護規劃，業依行政院訂頒「資安產業發展行動計畫（107－114 年）」辦理，依據 New eID 計畫經費至少 5%計算，經費約為 2 億 4 千萬元，範圍包含製卡中心、卡片、應用系統等面向。

一、印製作業安全(場地安全管理、晶片安全、資訊安全架構等)。

二、資訊安全系統架構(加密保護與傳輸方式、金鑰風險評估、系統防毒、弱點掃描等安全防護及測試)。

三、VPN 網路及系統硬體(點對點通訊加密、防火牆入侵偵測及防護、內網隔離及備援機制)。

四、系統軟體(導入第三方獨立驗證及確認，設置資安監控中心)。

五、運送保密安全(將 New eID 成卡安全運送至戶政單位)。

六、資訊安全教育訓練及系統安全進行稽核(辦理賞金獵人、資訊安全教育訓練，定期進行資安稽核)。

附錄一：內政部資訊系統委外服務案資訊安全管理規範

內政部資訊系統委外服務案資訊安全管理規範

一、廠商應遵循內政部（以下簡稱本部）資訊安全管理制度等相關規範，強化資訊安全管理，以確保資料傳送、儲存及流通之安全。

二、廠商應遵循與配合下列存取控制要求：

（一）禁止使用未經授權之網路設備及線路連結內部網路；如協助處理機密等級及限閱等級資料，應考量業務需求及資源可行性，決定是否採用專屬（隔離）之網路作業環境。

（二）避免使用共用帳號，如有特殊需求，須經機關之權責主管同意；因業務與資訊作業需求而使用資通訊設備或有帳號及權限異動需求者，應透過「帳號新增/異動申請表」進行申請及審核；如有因作業需求而持有系統管理員帳號，廠商應配合機關系統管理人員採取適當審核及確認作業。

三、廠商應遵循及配合下列運作安全要求：

（一）伺服器作業系統更新前，廠商應協助評估更新作業對應用系統之影響，或於測試環境測試無誤後再行申請更新作業；廠商進行開發、測試及線上運作之環境應設置於不同網路區段或資訊處理設施，以降低線上運作環境遭未經授權存取或變更之風險。

（二）廠商如需使用外來可攜式設備或媒體，應確認未遭受病毒感染。

（三）廠商應建立系統技術脆弱性資訊之取得管道，評估可能帶來之風險，並確認系統修正或安全問題更新程式之影響與處理方式。

（四）廠商應定期配合執行弱點掃描作業。

（五）系統須建置將使用者異動情形紀錄於稽核日誌之功能，且系統應提供查詢系統帳號之建立、修改、啟用、禁用及刪除動作、授予權限功能及異動紀錄。

（六）資訊系統應就涉及機敏資料部分建立稽核日誌，並確保資訊系統有稽核特定事件（至少包含更改密碼、登入成功及失敗、資訊系統存取成功及失敗）之功能，且僅限特定授權之使用者存取稽核日誌。

（七）稽核日誌需具備以下項目：

1.識別使用者之 ID，不可為個人資料類型。

2.時間應紀錄至秒等級。

3.執行功能或存取資源名稱。

4.執行結果或事件描述。

5.網路來源及目的位址。

（八）應用系統主機須建立時間同步機制。

四、廠商應遵循與配合下列通訊安全要求：

（一）若攜帶電腦或網路設備至本部，未經核准不得接入本部網路；禁止使用未經授權之網路設備、線路及私人電腦等設備連接內部區域網路。

（二）如有連線作業，須透過安全閘道（如：防火牆）或相關網路設備進行管控。

（三）未經許可不得以任何儀器設備或軟體工具進行網路通訊側錄、檢測及掃描；主機與網路設備連結之網路線不可隨意插拔、更換或接上其他非經允許使用之設備。

（四）如有常態性或定期資訊傳送作業，應述明交換內容、使用目的、範圍、風險控管等項目，經核可後始能辦理。

（五）執行電子傳輸前，機關及廠商須簽定保密協議文件，並依資訊機敏程度協議適當傳輸方式及安全保護措施（如：採行帳

號密碼管制、電子資料加密或電子簽章認證等）；如透過網際網路傳送機敏資料，應使用安全性連線方式傳輸（如：SFTP 及 HTTPS）或經由虛擬專用網路（VPN）處理，以確保資料隱密性；如透過專線傳送（如：封閉網路系統）機敏資料，應依資料安全等級，依相關安全規定適當加密處理。

（六）系統如有機敏資料存於資料庫或其他儲存媒體時，需採用對稱式或其他加密方式，將機敏資料加密成密文後儲存；傳輸機敏資料時，採用 HTTPS 等加密協定，確保機敏資料以密文方式傳輸。

五、廠商應遵循與配合下列密碼措施安全要求：

（一）廠商若使用憑證應用服務對訊息機密性、完整性、不可否認性、與可使用性之安全管控要求，應依據電子簽章法及其施行細則規劃與建置適當之亂碼化安全控管機制。

（二）系統加密方式，應採用公開、國際機構建議安全且未遭破解之演算法（如 AES 對稱式加密、RSA 非對稱式及 SHA-2 安全雜湊等演算法），並使用該演算法支援之最大金鑰長度，以減少被暴力破解解密之可能及弱點。

六、廠商應遵循及配合下列系統取得、開發及維護安全要求：

（一）廠商應參考現有系統或作業文件以進行應用系統開發、變更、增修需求之確認，瞭解現行作業流程，利用分析所收集到之資料，進行可行性與技術、作業執行及應用效益之評估，並應考量對現有資訊環境之影響。

（二）廠商應依據系統特性，規劃系統程式備份作業，並依據運作安全管理程序定期執行及驗證備份資料。

（三）廠商執行應用系統開發及維護之各階段活動時，宜參考「應用系統文件內容檢核表」產製相關文件。

（四）系統開發、變更及增修，應於需求分析階段即將資訊安全需求納入，並考量下列系統安全設計原則：

1. 系統應具備登入身分驗證機制，系統登入安全管理應參考存取安全管理程序設計。
2. 系統之設計應確保輸入與輸出資料、系統內部處理程序、系統與系統間資料介接、及系統紀錄訊息之資料完整性。

（五）對於字串之輸入應加以過濾或檢查，並限制前端應用程式資料輸入之長度及型別，並針對各輸入資料項目，規劃下列資料驗證功能：

1.是否超出輸入資料之設定範圍。

2.是否有錯漏之文字或數字。

3.是否有資料毀損或不正確。

4.是否有未經授權之資料或不一致之控制性資料。

5.過濾如「 ';"-- @ %」之類非預期之輸入字元。

（六）資料欄位之輸入為已知之資料範圍，應提供選單或選項之方式提供使用者輸入。

（七）有關機敏資料之輸入，應使用適當之遮罩或隱碼措施。

（八）系統應考量業務需求特性，設計使用者登入或連線逾時自動登出（以 15 分鐘以內為原則）或工作階段逾時（Session timeout）功能。

（九）應用程式應設計各種例外狀況管理（擷取和回傳例外狀況、設計例外狀況案例、傳送例外狀況資訊等）及處理機制，以利擷取及存錄錯誤資訊；並防止直接顯示原始完整錯誤訊息於終端使用者畫面。

（十）應用程式執行檔與暫存檔及其目錄應採取適當檔案保護措施（如：加密或存取限制）。

（十一）系統應考量資料重要性，針對重要功能作業（例如：登入、登出、資料刪除或變更等）留存軌跡紀錄。

（十二）機敏資料應在傳輸及儲存過程加密保護，並定期檢討加密機制之有效性。

（十三）應用系統開發及測試環境，應與正式線上環境區隔。

（十四）程式撰寫時應考量安全問題，避免出現已知弱點。

（十五）軟體開發生命週期中，考量開發方法之安全性，且建立使用各程式語言之安全開發指南。

（十六）系統開發完成後應進行測試，除測試系統功能外，亦應測試系統安全性。

（十七）開發人員應具備安全開發知識或接受相關訓練，以具備可避免、發現和修復脆弱性之能力。

（十八）若需轉移開發資料，應有適當安全傳輸機制。

（十九）廠商應進行程式碼安全檢測或程式碼檢視。

（二十）確認程式碼無論是新開發或變更，已由原始程式碼作者以外熟知程式碼檢查技術和安全程式碼實務之人員，參考業界安全程式碼標準檢視完竣。

（二十一）應用系統整合測試階段，應通過程式碼安全檢測（源碼掃描）或應用系統安全性檢測，並透過執行弱點掃描、滲透測試（黑箱測試）或應用程式安全掃描（白箱測試），檢查程式碼之安全性並修復至通過檢測。

（二十二）變更前需先進行必要之資料備份，以確保系統變更作業不致影響或破壞系統原有安全控制措施，以及變更失敗時可執行還原作業。

（二十三）廠商交付之系統，不得包含任何後門程式、隱密通道及特洛伊木馬程式等。

（二十四）系統須加強輸入檢核以防止 SQL Injection、XSS、篡改輸入等攻擊，並配合機關要求，在必要時協助建立 SQL Injection 與異常行為分析功能與報表；對於使用者輸入欄位資料，採用正規表示式（Regular Expression）進行檢查，僅允許輸入特定白名單內容，檢查其邏輯規則是否合法。

（二十五）系統需符合 IPV4 及 IPV6 協定。

（二十六）網站系統若具有與其他外部系統或資料庫之連線需求，不可將連線之身分驗證資訊（帳號、密碼等）寫於程式原始碼中，應採用設定檔或於系統啟動時動態輸入之方式。如以參數方式留存於設定檔，應確認僅有執行該系統之作業系統帳號可以存取設定檔。

（二十七）系統除了允許匿名存取之功能外，所有功能都必須已通過身分驗證才允許存取。網站除公開區域外，其他網頁皆需進行身分驗證登入成功後，才得以存取。系統傳遞身分驗證相關資訊（如：帳號、密碼等）應採用加密傳輸，不以明文傳輸，以避免資訊被攔截或監聽竊取。

七、廠商應遵循與配合下列供應商關係安全要求：

（一）廠商及其分包商於委外契約簽訂時，應與機關簽訂相關保密文件。

（二）廠商存取本部資訊處理設施或資訊時，應遵循法規與本部資訊安全管理制度，審慎評估其風險，採取適當控制措施。

（三）廠商若有下包廠商時，應要求其下包廠商亦應遵循本部資訊安全管理要求，必要時機關應審查廠商要求下包廠商之佐證資訊或文件。

（四）廠商所提供之服務若發生錯誤、中斷或資安事件，應留存相關紀錄，必要時機關應進行調查或稽核。

（五）廠商應配合機關資訊安全工作小組稽核分組不定期稽核資訊安全管理作業，或審查有關資訊安全之第三方外部稽核報告。

（六）廠商應配合機關專案承辦人員定期檢視與審查服務內容、報告及紀錄，以確保所提供之服務符合雙方協議同意等級。

八、廠商應遵循與配合下列資訊安全事故管理安全要求：

（一）廠商發現疑似資訊安全或個資外洩等異常事件或事故時，應負有即時通報機關資訊安全工作小組或個人資料保護管理小組，並提供事件或事故相關資訊之責任。

（二）廠商發現可疑之資訊安全事件、事故或安全弱點時（如：人員發現電腦使用異常情形、應用系統異常狀況告警、資訊機房管理人員發覺硬體設施、伺服器等設備發生異常狀況等）、或個人資料侵害告警事件或事故時，應立即以口頭、電話等方式通知本部資訊中心，本部資訊中心人員初判非屬一般維修情形，而為資訊安全/個人資料事件或事故後，應通報至事故通報處理分組。

附錄二：系統安全需求項目查檢表

系統安全需求項目查檢表

項次	分類	檢查項目	說明
1	1.機密性	1.1 機敏資料傳輸時,採用加密機制	說明：網站傳輸機敏資料時，採用 HTTPS（透過 TLS 等加密協定)協定以確保機敏資料以密文方式傳輸。
2		1.2 使用公開、國際機構驗證且未遭破解的演算法	說明：不使用自行創造的加密方式。採用公開、國際認可之演算法，例如 AES 對稱式加密演算法、RSA 非對稱式演算法及 SHA 安全雜湊演算法等。
3		1.3 使用演算法支援的最大長度金鑰	說明：系統中採用密碼學演算法時，使用該演算法目前支援的最大金鑰長度，以減少被暴力破解解密之可能及弱點。例如 AES256bits、RSA2048bits 或以上、SHA-512 等。
4		1.4 加密金鑰或憑證週期性更換	說明：產生網站 HTTPS 使用之憑證，應具備 3 年以下之使用年限限制，並於到期前進行更換。系統若另行使用自行產生之加密金鑰，亦需定期更換。
5		1.5 加密金鑰不與加密資料存放於同一系統中，並對於加密金鑰的存取進行限制	說明：常見加密金鑰以檔案形式放置於作業系統中，並以路徑存取，此作法之安全性較採用獨立之硬體安全模組（hardwaresecuritymodule，HSM）來保護金鑰為低。採用獨立之硬體安全模組，通常將金鑰保護於硬體晶片環境以避免被竊取，同時具備多種驗證類型(IP、PIN 碼等），對金鑰存取進行限制。（加密金鑰不與加密資料存放於同一系統中，並對於加密金鑰的存取進行限制）
6		1.6 機敏資料儲存時,採用加密機制	說明：機敏資料存於資料庫或其他儲存媒體時，採用對稱式或其他加密方式，將機敏資料加密成密文後儲存，並於需要取得原文明文時解密還原。此作法可減少機敏資料因儲存媒體有其他存取管道而洩漏的風險。

項次	分類	檢查項目	說明
7	2.完整性	2.1 於伺服器端以正規表示式（RegularExpression）方式，檢查使用者輸入資料合法性	說明：對於使用者輸入欄位資料，於伺服器端採用正規表示式（RegularExpression）進行檢查，僅允許輸入特定白名單內容，檢查其邏輯規則是否合法。
8		2.2 針對開放下載的資料，也提供資料之雜湊值（HASHValue）供使用者比對其完整性	說明：網站提供使用者下載的資料，於下載連結處，以安全雜湊演算法產生雜湊值（HASHValue）供使用者參考比對，並說明使用的雜湊演算法為何。
9		2.3 具有防範 SQL 命令注入攻擊（SQLInjection）之措施	說明：系統於伺服器端具有防範 SQL 命令注入攻擊措施。例如，Preparedstatements、Storedprocedures 、輸入驗證（InputValidation）等。
10		2.4 具有防範跨站腳本攻擊（Cross-SiteScripting）之措施	說明：系統於伺服器端具有防範跨站腳本攻擊（Cross-SiteScripting）措施。例如黑名單過濾跳脫特殊字元、白名單正規表示式驗證、輸出編碼等。此安全需求項目僅適用於 WEB 網站系統。
11		2.5 驗證網頁重導（Redirects）與導向（Forwards）之目的地在合法名單內	說明：網站若提供網頁重導或導向之功能，必須確認使用者輸入欲重導向的網頁，其值在合法白名單內，以避免被利用來重導向至惡意網頁。此安全需求項目僅適用於 WEB 網站系統。
12		2.6 重要系統資料或紀錄留存雜湊值以確保完整性	說明：重要資料或紀錄，以安全雜湊演算法產生並留存其雜湊值，後續可對資料再次產生雜湊值並與原先結果進行比對，以確保資料未遭到異動竄改。
13	3.可用性	3.1 重要資料定時同步至備份或備援環境，並加以保護限制存取	說明：系統具備重要資料定時備份機制，依組織規範將資料同步至備份或備援環境，以避免系統毀損或資料綁架勒索對資料可用性之危害。重要資料於備份或備援環境應有保護限制存取措施，以避免增加其他資安風險。
14		3.2 採用「高可用性」（HighAvailability）架構（分散式或叢集伺服器架構）	說明：系統之服務水準，經評估後須滿足高可用性需求者，應考量採取分散式或叢

項次	分類	檢查項目	說明
			集伺服器架構，以使當系統發生錯誤情況或硬體毀損時，服務仍能正常運作。
15	4.身分驗證	4.1 除了允許匿名存取的功能外，所有功能都必須已通過身分驗證才允許存取	說明：網站除公開區域外，其他網頁皆需已進行身分驗證登入成功後，才得以存取（接續應檢查該使用者權限是否允許其存取該網頁或功能）。使用者若存取非公開區域，檢查機制發現其尚未通過身分驗證時，應不允許其存取頁面並將其導向至首頁或登入頁面。
16		4.2 身分驗證機制位於伺服器端且採用集中過濾機制（例如使用 Filter 過濾器）	說明：系統應包含具有一致全面性、位於伺服器端，強制適用於全系統的授權及存取控制機制。例如使用 Filter 過濾器機制。
17		4.3 身分驗證相關資訊（帳號、密碼等）不留存於程式原始碼中	說明：網站系統若具有與其他外部系統或資料庫等連線的需求，不可將連線之身分驗證資訊（帳號、密碼等）寫於程式原始碼中，應採用設定檔或於系統啟動時動態輸入之方式。身分驗證資訊若以參數方式留存於設定檔，應確認僅有執行該系統之作業系統帳號可以存取設定檔。
18		4.4 確實規範使用者密碼強度（密碼長度 12 個字元以上、包含英文大小寫、數字，以及特殊字元）	說明：若採用密碼作為身分驗證機制，當使用者設定密碼時，需以正規表示式檢查密碼強度是否符合標準，例如密碼長度 12 個字元以上、包含英文大小寫、數字，以及特殊字元。
19		4.5 使用者必須定期更換密碼，且至少不可以與前 5 次使用過之密碼相同	說明：使用者初次設定或異動密碼時，系統應留存設定密碼之時間，往後每次使用者成功登入後，必須檢查該組密碼是否已使用超過組織政策所規定的最長期限（例如，45 天），若已超過時限則強制使用者更換密碼，使用者的前 5 次舊密碼應被保留（以雜湊值的形式），新密碼應比對且不允許與前次使用密碼相同。

項次	分類	檢查項目	說明
20		4.6 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 3 次後，至少 30 分鐘內不允許該帳號及來源 IP 繼續嘗試登入	說明：系統須具備帳戶鎖定機制，紀錄使用者身分驗證錯誤次數，若錯誤次數達到組織資安規範之次數（例如，3 次），則針對該帳號及來源 IP 進行鎖定一段時間（例如，30 分鐘）。鎖定時間後使用者再次進行身分驗證登入嘗試時，應將錯誤次數歸零。除帳號外亦鎖定來源 IP 的用意為防範攻擊多個帳號，使同一來源無法在某個帳戶鎖定後，又再行嘗試其他帳戶。
21		4.7 身分驗證相關資訊不以明文傳輸	說明：系統傳遞身分驗證相關資訊（例如帳號密碼）時，採用加密傳輸，以避免該資訊被攔截或監聽竊取。
22		4.8 密碼添加亂數（Salt）進行雜湊函式（HASHFunction）處理後，分別儲存亂數及雜湊後密碼	說明：系統儲存使用者密碼時，不宜儲存明文密碼，以避免遭到有心人士竊取。使用者設定密碼時，應針對該使用者產生一個亂數值，將使用者密碼結合亂數值，再以雜湊函式（HASHFunction）處理產生雜湊值後，分別於不同欄位儲存使用者亂數值及雜湊值。後續使用者輸入密碼時，以輸入值添加當初設定密碼時產生的亂數，再次以雜湊函式處理，若產出結果同當初設定密碼時的雜湊值，則表示輸入密碼正確。
23		4.9 採用圖形驗證碼（CAPTCHA）機制於身分驗證及重要交易行為，以防範自動化程式之嘗試	說明：系統若採用帳號密碼進行身分驗證，往往可能遭受到自動化程式以暴力破解方式嘗試登入。另外，系統重要行為若被獲知相關執行參數，亦可能被自動化程式嘗試偽冒合法使用者觸發。因此，採用圖形方式顯示一驗證碼於頁面上，並要求使用者辨別該圖形中文字之方式，或以其他足以辨識人為動作之方式（例如勾選特定選項），將可以防堵自動化程式之嘗試行為。
24		4.10 重要交易行為要求使用者再次進行身分驗證	說明：系統中重要交易行為，於執行前應再次確認獲得授權。要求使用者再次身分驗證是確認獲得授權的手段之一。另外此作法亦可有效防堵攻擊者透過其他方式

項次	分類	檢查項目	說明
			取得使用者身分憑證後，直接偽冒使用者執行重要交易行為。
25		4.11 採用多重因素身分驗證（兩種以上驗證類型）	說明：系統身分驗證或重要交易行為，可採用多重因素身分驗證以強化安全性。多重因素身分驗證意指具備兩種以上驗證類型，驗證類型一般區分為所知之事（Somethingyouknow）、所持之物（Somethingyouhave）及所具之形（Somethingyouare）。所知之事類型常採用密碼、特定問題之答案等。所持之物類型常採用令牌（Token）、憑證、簡訊、電子郵件等。所具之形類型常採用生物特徵，如指紋、虹膜辨識等。
26		4.12 密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性令牌（Token），檢查傳回令牌有效性後，才允許使用者進行重設密碼動作	說明：密碼重設機制設計不良可能造成安全問題。常見錯誤是系統主動將密碼重新設定後寄送給使用者。使用者忘記密碼並啟動密碼重設機制時，應以使用者其他留存於系統的聯絡資訊，例如電子郵件或手機號碼，先要求使用者輸入該資訊，比對正確無誤後，發送一次性及具有時效性令牌（Token），一般是亂數產生的英數字，使用者接收後須於時效內進行輸入回傳動作，系統檢查回傳令牌有效性後，允許使用者重設密碼。
27	5. 授權與存取控制	5.1 執行功能及存取資源前，檢查使用者授權	說明：系統中除了公開區域外，任何執行功能及存取資源動作前，應檢查使用者已通過身分驗證且使用者具備權限可執行該功能或存取該項資源。
28		5.2 採用伺服端的集中過濾機制檢查使用者授權	說明：檢查使用者是否具備存取功能或資源之機制，應位於伺服器端且採用全面性集中控管機制(例如採用網站過濾器 Filter 機制），明確設定檢查範圍。檢查機制位於伺服器端可以避免被攻擊者繞過檢查的問題，全面性集中控管可以避免人為疏漏導致可能有功能未檢查使用者授權之問題。

項次	分類	檢查項目	說明
29		5.3 對使用者/角色，僅賦予所需要的最低權限	說明：明確定義系統中角色及對應的權限，系統上線驗收時，應審查使用者賦予的角色及其取得的權限是否適當，系統上線後亦定期審查使用者所擁有的角色與權限清單。相關資訊宜提供系統介面以供查詢或匯出。
30		5.4 軟體程序（process）及伺服器服務，以一般使用者權限執行，不以系統管理員或最高權限執行	說明：系統之軟體程序或伺服器服務，若以系統最高權限或管理員權限啟動，將造成攻擊者成功入侵伺服器時，可以取得作業系統最高權限。應於作業系統增加服務專用之使用者，並授予執行伺服器服務及讀寫相關檔案的有限範圍權限，使其可以正常執行軟體程序作業，同時避免過高權限之風險。
31		5.5 除特殊管理者權限外，其他角色或權限無法修改系統中授權資料及存取控制列表（ACL）	說明：存取控制列表是用來表示系統使用者具有哪些權限的清單，實際上可能由多張表格組成，包含使用者清單、角色清單、權限清單、角色與權限關聯清單及使用者與角色關聯清單等。系統應確保只有特定管理員權限可以透過介面或具備資料庫權限可以修改存取控制列表，一般使用者無存取控制列表之修改權限。
32		5.6 重要行為由多人/角色授權後才得以進行	說明：設計軟體功能時將條件設定在兩個或多個以上，且需要滿足所有的條件才能完成作業時，稱之為職責分離（SeparationofDuties）。系統重要行為可以採取須通過多人/角色授權後才得以進行之設計。職責分離可以減少單一人員或資源由於權限過大，所可能造成的安全危害。實行職責分離再加上行為的稽核紀錄，可以防範內部舞弊的情況發生。
33		5.7 具有防範「跨站請求偽造」（Cross-SiteRequestForgery，CSRF）攻擊之措施	說明：「跨站請求偽造」攻擊發生情況為，攻擊者知道網站特定行為的執行參數，在使用者已通過網站身分驗證登入後，以欺騙使用者點選連結或其他方式，偽造使用者之請求進行該特定行為並帶入相關參數，以遂行惡意之目的。防範 CSRF 的措施主要有：1.重要行為前先動態產生獨立

項次	分類	檢查項目	說明
			而唯一的 requesttoken，並於執行行為前檢查。2.要求使用者重新身分驗證或證明該動作是人為進行（使用 CAPTCHA）。此安全需求項目僅適用於 WEB 網站系統。
34	6.日誌紀錄	6.1 針對身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為進行日誌紀錄	說明：系統留存日誌紀錄之目的包含程式除錯、行為歸責、稽核取證及法規要求等。紀錄身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等，將有助於定期稽核系統行為及資安事件追查。
35		6.2 日誌紀錄包含以下項目： 1.識別使用者之 ID（不可為個資類型）。 2.經系統校時後的時間戳記。 3.執行的功能或存取的資源。 4.事件類型或等級（priority）。 5.事件描述	說明：日誌紀錄宜考慮包含： 1.使用者 ID，不可為個資類型，避免共用帳號之情。 2.時間，系統應設定定期校時，應紀錄至微秒等級。 3.執行之功能或存取之資源名稱。 4.事件類型或優先等級。 5.執行結果或事件描述。 6.事件發生當下相關物件資訊。 7.網路來源與目的位址。 8.錯誤代碼，便於事件追查。
36		6.3 採用單一的日誌紀錄機制，確保輸出格式的一致性	說明：系統日誌紀錄應盡可能採用單一的 Log 機制，例如同一伺服器軟體應產出相同格式之日誌紀錄，以便於事件比對與追查。
37		6.4 對日誌紀錄進行適當保護及備份，避免未經授權存取	說明：系統產生日誌紀錄後，應定時將日誌紀錄進行遠端備份，並將檔案設定存取權限限制，避免未經授權存取。
38	7. 會談（Session）管理	7.1 使用者的會談階段，設定該帳號在合理的時間（至多 30 分鐘）內未活動即自動失效	說明：會談（Session）機制目的為管理使用者與伺服器之間的連線狀態，通常於客戶端首次連線伺服器即建立一會談識別碼（SessionID），並將使用者後續於系統中的相關資訊與該會談識別碼關連，以維持使用者相關資訊狀態。使用者於系統中若一段時間未進行活動，系統應有自動機制將該使用者的會談階段設為失效，以避免資安風險。

項次	分類	檢查項目	說明
39		7.2 使用者的會談階段在登出後失效	說明：系統應有手動機制，使用者明確進行登出後，將該使用者的會談階段設為失效。
40		7.3 會談識別碼(SessionID)或使用者 ID 避免顯示於使用者可以改寫處（例如網址列）	說明：會談識別碼（SessionID）顯示於使用者可以改寫處，則有遭到暴力破解或嘗試猜測合法會談識別碼之可能性，應予避免。
41		7.4 會談識別碼(SessionID)採亂數隨機產生且不可預測	說明：為避免會談識別碼（SessionID）被猜測，建議儘量使用各種開發架構(J2EE、ASP.NET、PHP）所提供的內建 SessionID 產生管理方式，而不要自己產生 SessionID，以確保 SessionID 具隨機性與夠強健而不易被推測。
42		7.5 使用者登入後，重新賦予會談識別碼（SessionID）	說明：針對會談識別碼（SessionID）的 SessionFixation 攻擊，攻擊者在目標使用者登入前置換掉其所使用的 SessionID，使用者登入後將取得系統權限，攻擊者利用其已知的這組 SessionID 便可以偽冒成目標。伺服器在使用者初次連結網頁時（通常為首頁）給予 SessionID，登入後若仍採用相同 SessionID 則具有此風險。
43	8. 錯誤及例外管理	8.1 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息	說明：系統應設計錯誤處理機制，當系統發生錯誤時，儘可能採取錯誤代碼或簡短訊息呈現，避免將詳細或除錯用訊息直接顯示於使用者頁面，以防被攻擊者用來刺探系統內部資訊，或根據錯誤訊息推測出系統可能之弱點。
44		8.2 所有功能皆進行錯誤及例外處理，並確保將資源正確釋放	說明：確保系統所有功能的程式碼，在程式的進入點之後，盡可能採用程式語言的 try-catch 陳述，捕捉可能發生的錯誤與例外狀況。另外，採用程式語言的 finally 陳述，確保將該段功能程式碼所使用的資源正確釋放。

項次	分類	檢查項目	說明
45		8.3 具備系統嚴重錯誤之通知機制（例如電子郵件或簡訊）	說明：系統增加電子郵件或簡訊之通知機制，並就系統錯誤或例外狀況進行等級區分，當嚴重等級錯誤發生時，採用通知機制，使系統管理員或相關人員得以即時得知錯誤發生，進行後續處理。
46	9.組態管理	9.1 管理者介面限制存取來源或不允許遠端存取	說明：管理者介面通常可執行系統中較高權限的功能（例如權限與人員管理），其相對風險較高，因此應盡可能不允許遠端存取，僅允許透過內部網路存取，以避免有心人士從外部嘗試攻擊之可能。若有必要允許外部遠端存取管理者介面，應限制特定存取來源 IP，避免全面性開放存取。
47		9.2 作業平台定期更新並關閉不必要服務及埠口（Port）	說明：就作業系統或平台之安全更新，定期評估、測試與更新。系統上線前，就作業系統或平台預設開啟的服務與埠口（Port）進行檢視與評估，盡可能關閉不必要之項目，並正面表列需要開啟該服務及埠口（Port）之理由。
48		9.3 系統依賴的外部元件或軟體，不使用預設密碼	說明：表列系統所使用的外部元件與軟體，包含其版本資訊，並檢核確認未有使用預設密碼之情況。
49		9.4 參數設定或系統設定存放處，限制存取或進行適當保護	說明：系統參數設定檔案，應設置適當檔案權限，避免被非授權存取。
50		9.5 針對系統依賴的外部元件或軟體，注意其安全漏洞通告，定期評估更新	說明：對系統所使用的外部元件與軟體進行表列，包含其版本資訊。注意相關之安全漏洞通告（透過 CVEDetails 網站、廠商安全通告等），於系統驗收前確認採用之軟體與元件，已使用最新之穩定版本或該版本已排除所有已知安全漏洞。系統上線後，持續定期關注安全漏洞通告，若有相關之安全漏洞發生，評估該系統元件更新之必要性，於系統測試環境進行更新測試驗證後，才於正式環境進行更新。

附錄三：內政部委外服務案個人資料保護規範

內政部委外服務案個人資料保護規範

一、機關委託廠商蒐集、處理或利用個人資料及檔案時，應遵守本規範相關規定。

二、蒐集、處理或利用時之義務

（一）廠商依契約規定蒐集、處理或利用個人資料時，應遵守個人資料保護法、該法施行細則及內政部（以下簡稱本部）個人資料保護管理制度等相關規定。

（二）廠商不得利用機關提供或履行契約蒐集之個人資料及檔案，為自己或他人利益從事契約履約目的範圍以外之處理或利用行為，或以任何方式或方法交付予履約無關之第三人。

（三）廠商僅得於機關以下指示之範圍內，蒐集、處理或利用個人資料：

■預定蒐集、處理、利用

範圍：新一代國民身分證換發系統建置及維護案

蒐集資料：處理戶役政業務及自然人憑證業務所蒐集之相關個資

期間：本案履約期間

□其他：

三、安全（維護）措施

廠商在履行契約所必須之範圍內，應依個人資料保護法第二十七條第一項規定採行個人資料保護法施行細則第十二條所規定適當之安全（維護）措施。

四、複委託之約定如下：

□機關及廠商約定複委託予第三人執行時，廠商負有下列義務：

(一) 廠商履行契約前，就涉及蒐集、處理或利用個人資料或檔案之業務擬複委託予第三人執行者，應提出受複委託第三人之名

稱、地址、符合第二點第三款之執行業務範圍、對該第三人設置之監督機制及保密同意書等文件，經機關審查通過，並以書面同意後始得辦理。

(二) 廠商應依第二點規定限定受複委託第三人蒐集、處理、利用個人資料之範圍，並對該受複委託第三人依個人資料保護法及本部個資保護管理制度等相關規定進行適當之監督。

(三) 受複委託第三人於委託範圍內蒐集、處理、利用個人資料之行為，視同廠商行為，廠商應負所有責任。

□廠商執行契約，就涉及蒐集、處理或利用個人資料或檔案之業務，不得複委託第三人執行。

五、當事人權利行使時之義務

機關受理當事人依個人資料保護法第三條規定行使當事人權利時，廠商應於機關指定期限內，配合提供資料或提出說明；當事人如逕向廠商或受其複委託第三人行使個人資料保護法第三條所定權利者，廠商或受其複委託第三人除應依相關規定辦理，並應於三十日內將處理情形以書面通知機關備查。

六、配合義務

（一）廠商依個人資料保護法第十五條第二款或第十六條但書第七款規定，經當事人同意而為蒐集、處理或特定目的外利用前，應將該同意內容與取得方式送交機關審查。廠商依個人資料保護法第六條第一項第六款規定，經當事人書面同意而為蒐集、處理及利用者，亦同。

（二）機關於契約期間內，得要求廠商提供或說明涉及個人資料業務之處理事項，並提供相關資料，廠商不得拒絕。

（三）必要時，機關得要求廠商於簽約後一個月內參考機關個人資料保護相關規範，訂定「個人資料保護專案計畫書」送機關

備查，計畫書中應包含個人資料保護法令及機關要求之安全維護事項。若有變更計畫內容，應函送機關備查。

七、個人資料事故通知義務

廠商因履行契約，致個人資料被竊取、洩漏、竄改或其他侵害之情形時，於發現後，應立即通知本部，並採取因應措施；廠商於查明後應將其違反情形、涉及個人資料範圍、採行及預定採行之補救措施通知本部，經本部同意後，依法以適當方式通知當事人。

八、定期確認

（一）機關得針對廠商個人資料安全管理措施實施情形進行審查，並將審查結果作成紀錄備查；必要時，得派員進行實地訪查或委託專業人員進行查核，廠商應予配合。

（二）機關於訪查或查核後，認有缺失，得以書面敘明理由通知廠商限期改善。

九、損害賠償責任

（一）廠商違反本規範第二點至第七點、第八點第一款、第十點或經機關依第八點第二款限期改善而屆期未改善，機關得依契約規定處理；若機關受有損害，並得請求損害賠償。

（二）廠商因履行契約而有違反個人資料保護法、個人資料保護法施行細則等規定，致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。

（三）機關因廠商履行契約違反個人資料保護法或其施行細則而受有損害時，得向廠商請求損害賠償。若因此遭第三人請求損害賠償時，應由廠商負責處理並承擔一切法律責任；如於訴訟中，廠商應協助機關為必要之答辯及提供相關資料，並應負擔因此所生之訴訟費用、律師費用及其他相關費用，並負責清償機關對第三人所負之損害賠償責任。

十、履約中或契約終止時資料之刪除或返還

（一）除機關、廠商雙方另有約定或法律另有規定外，廠商應於履約期限屆滿或經機關要求時，將因履行契約而取得之個人資料及檔案全數返還予機關，其備份應全數銷毀刪除，不得以任何形式自行留存、保留存取權限或提供予第三人利用；並提供刪除、銷毀或返還個人資料之時間、方式、地點等紀錄備查。

（二）前款返還，廠商得向機關指定之第三人交付之。

十一、 第一款刪除、銷毀作業，廠商應於作業前一日通知機關，機關得於必要時派員進行實地查訪或委託專業人員進行查核，廠商應予配合。

附錄四：名詞定義

一、身分驗證：當事人之身分透過面對面或線上進行檢驗及查證。

二、資料驗證：針對當事人提供之資料進行檢驗及查證。

三、內政部授權：由內政部授與權限使之可以進行讀取晶片。

四、非經授權：並沒有經過授與權限。

五、取得認證：針對各項國際標準得到相關證書。

六、卡片：係為空白卡（含晶片）、半成卡、成卡、壞卡、報廢卡之統稱。

七、空白卡：係指卡廠未經資料填寫或植入等處理之卡片。

八、晶片：係指為製作 New eID 之晶片。

九、廢卡：係指壞卡以及報廢卡。

十、壞卡及報廢卡：製卡人員於製卡前，發現空白卡（含晶片）品質有問題，即為壞卡，無問題者則辦理空白卡初始化程序及印製作業。印製完成後，發現成卡品質不佳，即為報廢卡。

十一、瑕疵卡：指卡片印製完成送至戶政事務所，戶政事務所發現成卡品質不佳，即為瑕疵卡。

十二、非瑕疵之作廢卡：指成卡送至戶政事務所後，戶政事務所發現有不予發卡予當事人情形(如出境戶籍遷出、死亡、受死亡宣告、廢止戶籍登記或撤銷戶籍)或當事人因換證而回收之舊卡等，此種非因卡片本身瑕疵而作廢卡片，即為非瑕疵之作廢卡。

十三、卡廠：係接受內政部委託之製卡中心為生產所提出採購 New eID 空白卡（含晶片）之廠商。

十四、製卡中心：指集中製證場所，係由內政部委託從事卡片個人化作業及封裝等事宜，並向卡廠提出採購 New eID 空白卡（含晶片）需求之單位。

十五、New eID 管理系統：係指將申請資料與戶役政系統及憑證系統連結提供製卡中心製作 New eID，並控管 New eID 從申請到製證及發放等事宜，就 New eID 生命週期進行管理。

十六、New eID 應用程式介面（以下簡稱 API）：係指得以整合及介接 New eID 公開區及加密區資料之程式，包含用以交換資訊之函式或應用服務等及其他內政部認可之應用程式介面。

十七、業務應用系統：需用機關整合 New eID API 之業務應用系統。

十八、全面換證對象：本計畫換證對象為在國內設有現戶戶籍之現住人口。但不包括矯正機關收容人，矯正機關收容人於出矯正機關後，再向戶政事務所申請 New eID。出境戶籍遷出國外人口，辦理遷入登記時，同時向戶政事務所申請 New eID。

十九、全面換證製程期間：係指戶政事務所依所轄村（里）、鄰人數，自排定轄內人口換證期程至完成換證之期間。於此期間，申請人除因初領、補領、辦理戶籍登記同時須換領國民身分證，不得提前申請新證。

二十、數位身分識別證（New eID）：指國民身分證附加自然人憑證。

二十一、用戶代碼：為英數字 6-10 碼，可使用於設定 New eID 加密區及自然人憑證之初始密碼、或當加密區及自然人憑證密碼忘記或被鎖卡，可用以重新設定密碼，另當要線上停（復）用自然人憑證時，需輸入用戶代碼。

二十二、讀取碼：用以讀取公開區，為卡片序號後 6 碼。

二十三、PIN1：指加密區使用之密碼，為數字 6 碼，於輸入 PIN1 時，可讓經內政部審定之第三方讀取加密區欄位。

二十四、PIN2：指自然人憑證使用之密碼，為數字 8-12 碼，於輸入 PIN2 時，可使用於網路身分識別及電子簽章功能。