序　言

本報告書係為「新一代國民身分證換發規劃案」廠商交付之成果報告書（以下稱廠商報告書），僅作為本部辦理新一代國民身分證換發作業政策參考之用，部分內容業與本部參考各界資安強化意見及實務狀況所調整完成並公開之**「規劃成果重點報告（以下稱本部報告書）」有所不同**，合先述明。

主要差異說明如下：

(一)廠商報告書原規劃「晶片存放自然人憑證，民眾可選擇關閉啟用自然人憑證功能」，調整為「民眾可選擇是否附加自然人憑證」。

(二)廠商報告書原規劃「公開區讀取碼為國民身分證統一編號後 6 碼」，調整為「卡片序號後 6 碼」。

(三)廠商報告書原未規劃小規模試行全面換證，新增規劃小規模試行，擇定部分縣市試行 3 個月或半年，並辦理賞金獵人競賽，開放民間團體進行黑箱測試，爭取民眾信任。

(四)廠商報告書原規劃「晶片 ICAO 區寫入資料」，調整為「關閉晶片 ICAO 區」。

(五)廠商報告書原規劃「晶片加密區及自然人憑證區自訂密碼長度同樣為 6-12 碼數字」，調整為「晶片加密區自定密碼長度 6 碼數字；自然人憑證區自訂密碼為 8-12 碼」，以確保民眾不會設定相同密碼，該 2 區也由可雙界面讀取，調整成僅可以接觸式讀卡設備讀取。

(六)廠商報告書中有關 API 應用程式規劃之內容多涉及技術面之說明及程式函式定義等，經綜整確認名詞及新一代國民身分證換發工作小組第 4 次會議決議，將本部報告書內容調整為較淺顯易懂之內容及文字。

(七)廠商報告書中有關自然人憑證方案比較，經政策確認後，僅保留採行之方案列於本部報告書中。

(八)考量資安兼具便民原則下，有關自然人憑證效期，廠商報告書原規劃 5 年，可「展期」5 年，本部報告書調整為 5 年，可「更換金鑰」之後再用 5 年共 10 年。

(九)廠商報告書規劃行動臨時身分證 APP 及行動身分證部分，須俟數位身分證各項工作完善，並確保安全無虞後再推動，相關段落先行刪除避免造成誤解。

(十)廠商報告書有關委託運送管理規範或準則部分，後依據實務於本部報告書中調整。

(十一)本部報告書中增加整體架構資訊安全相關規劃專章。

內政部

新一代國民身分證換發規劃案

成果報告書

V 2.0

國巨管理顧問股份有限公司

中華民國 108 年 12 月 13 日

目錄

表目錄

圖目錄

第壹章、專案概述

壹、專案緣起

內政部刻正辦理數位身分識別證（簡稱 New eID）換發事宜，New eID 初步規劃為晶片卡設計，將個資揭露最小化，版面公開個資降至最低，晶片內存放現行紙本身分證相同之個人資訊及自然人憑證，使其具有網路身分識別功能，並可由民眾依其意願決定憑證使用狀態（停、復用或廢止），讓 New eID 成為開啟智慧政府之鑰，達成智慧政府便捷智能服務、倍增服務效能及永續透明治理之目標。

為完善規劃新一代國民身分證全面換發工作、後續營運及各項應用，委託國巨管理顧問股份有限公司(以下簡稱本團隊)辦理「新一代國民身分證換發規劃案」（以下簡稱本案）。

本案自簽約日起至 108 年 11 月 30 日止，另於本案履約期間，協助辦理「新一代國民身分證換發建置案」公開閱覽程序及提供技術諮詢。

本報告係針對本案提出原則性規劃建議，實際狀況應由內政部視具體情況及實務需求進行調整。

貳、工作項目

本團隊依契約於專案期間應執行以下工作項目，各項工作內容如有不足或異動之處，應依內政部需求配合修正規劃內容，各項工作說明如下：

一、卡片（含晶片）規格及需求規劃

New eID 採用之空卡（含晶片）規格、卡片防偽變造設計並提供 30 張樣卡、卡片（含晶片）安全防護措施、卡片耐用性、抗彎曲、耐磨、防水、抗污、耐高溫等規格、晶片存取設計（接觸及非接觸式）、New eID 式樣及印製內容、臨櫃取像規格及方式、成本及規費

分析、製證期間 New eID 替代方案（如臨時身分証明之防偽設計）、當晶片失效時卡片是否有效之評估、卡片與憑證之效期及如何配合、規劃應用展示區（民眾體驗各種應用情境）、換卡潮配套機制。

二、製卡中心規格、管理規範及安全規劃

New eID 製證場所規格與地點評估、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，製證設備、耗材、廢料處理、品管機制）、不同階段之成本分析（全面換發、後續維運、屆期換卡），人力及管理規劃、資安防護規範。

三、製發管理規劃

New eID 採購、製程、印製作業、資料及憑證寫入作業、產品庫房管理、產品封裝檢測、委託運送及耗材管制等管理規範或準則、流程及安全控管機制、成卡品質需求（如文字格式、影像亮度、膠膜封裝良率、彩度及對比等規範）及控管規範、製發管理系統軟硬體規格及與現有系統介接整合規劃（戶役政系統及自然人憑證中心）、備援及復原機制規劃。

四、API 應用程式規劃

API 介接應用服務管理系統軟硬體規格及功能、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，支援目前作業系統版本包括個人電腦的 WINDOWS、LINUX、MAC 平台，以及智慧型手機的 IOS、ANDROID 平台）、API 客戶服務中心人力及管理規劃、介接系統資訊安全及個資保護機制、應用系統使用紀錄及軌跡稽核、產官學研申請介接系統規範及輔導維運。

五、新身分證應用軟體規劃

（一）個人端維護軟體規劃：提供於個人電腦與手機執行之軟體規劃（至少包括檢視新身分證登載資料、變更密碼及線上憑證展期、補換卡申請作業）、讀卡機及相關設備規範(含接觸及非接觸式)、資安防護規範。

（二）機關端應用軟體規劃：提供機關檢視新身分證個資（戶籍地區、公開區、加密區個人資料）及卡片有效性（比對廢卡清單）之軟體規劃、讀卡機及相關設備規範（含接觸及非接觸式）、資安防護規範。

（三）行動身分證軟體規劃：供民眾臨櫃使用，民眾以 New eID 綁定手機，可在不攜帶 New eID 情況下，以手機顯示動態條碼，驗證機關讀取動態條碼後，連結至後端資料庫取得民眾資料身分證資料。

六、規劃新身分證之晶片內容遠端更新之作法

規劃 New eID 之晶片內容遠端更新之作法,並評估其資安風險。另規劃行動 eID 之配套措施(包含與民間業者配合之可行性評估)。

七、自然人憑證規劃

（一）應就 New eID 所使用之自然人憑證，應採新建發證系統或整合現行自然人憑證發證系統，或其他更好可行方案，及其衍生之相關議題，進行詳細規劃評估，並交付相關規劃報告。內容包括：

1. 法規調適及憑證實務作業基準修訂。

2. 新舊憑證如何區分?並存?或取代?如何移轉等議題。

3. 憑證效期及換發作業規劃。

4. 憑證中心及卡管中心規範與備援機制規劃。

5. 憑證發證系統、卡管系統、製卡系統、及戶役政系統間之介接方式及標準規範。

6. New eID 晶片採用之中介軟體，如 CSP（PKCS#11），APPLET（PKI）等，及載具機制，除須考量現行自然人憑證之相容性，應規劃為共用標準，使未來可適用各廠牌之晶片。

7. 晶片效能標準規劃。（ICAO、PKI APPLET PERFORMANCE）

8. 提供金鑰載具中金鑰對演算法及功能規劃：

(1) 提供金鑰載具中金鑰對演算法及功能規劃，比如使用 ECC-384 或 RSA-2048 或同等級以上之金鑰對，一對用於數位簽章，另一對用於加解密或金鑰交換之用等。

(2) 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。

(3) 提供憑證更新、展期、線上操作規劃。

9. 分案建置或 1 案建置（證卡分離）規劃。

10. 憑證應用 API 規劃：

(1) 提供應用安全保密函式庫規劃，以利機關單位或組織團體快速開發憑證應用系統。

(2) 提供 API 支援目前作業系統版本規劃，例如：個人電腦的 WINDOWS、LINUX、MAC 平台，以及智慧型手機的 IOS、ANDROID 平台。

(3) 提供跨平台網頁元件規劃，以支援現行各主流瀏覽器操作環境。

(4) 函式庫須能支援自然人憑證卡片等相關載具。

(5) 函式庫功能應包含數位簽章、驗章、加解密、憑證解析、憑證驗證、憑證廢止狀況查詢，以及 IC 卡操作等應用。

(6) 函示庫提供用戶身分識別碼設定、重置及行動化裝置綁定功能。

11. 自然人憑證身分認證等級及載具安全等級標準規劃：規劃身分認證與載具安全的保證等級標準以及各保證等級的選用方式，供民眾與各應用服務身分認證等級採用標準之參考，民眾或各類應用依其可承受的風險選用不同認證強度的保證等級，等級越高，可信賴度越高，身分認證亦越嚴謹，透過身分認證的等級分類，可省略不必要的認證流程，提升認證的效率及可信賴度，促進身分認證機制健全發展。

（二）其他可能涉及之議題規劃。

八、先期作業期間 New eID 宣導資料規劃及製作

製作先期作業期間之宣導資料，可以影片（或動畫）、懶人包、海報或其他創新行銷方案（應符合預算法第 62 條之 1 規定），讓全民能充分了解 New eID 換發內容及效益，並以活潑易懂的方式向民眾說明 New eID 內容及相關配套措施，使各界能充分了解計畫內容並化解諸項疑慮，營造社會良性溝通及凝具全民共識。

九、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

（一）規劃 New eID 換發網站，對外提供 New eID 換發內容及 QA 說明等網頁。

（二）規劃於換發期間之 New eID 宣導資料（應符合預算法第 62 條之 1 規定）。

（三）規劃於換發期間對戶所人員之教育訓練課程。

十、各項標準作業程序（SOP）

（一）New eID 印製及品質控管：規劃空白晶片身分證初始化、卡面資料印製、相片影像印製、憑證寫入等作業功能流程、品管及安全機制。

（二）New eID 空白卡及製發安全控管（廢料及廢卡控管、成卡庫存）：規劃空白晶片身分證之原物料採購、控管、製程安檢、產品庫房安全管理、委託運送及耗材安全管制等生產與管理規範或準則。

（三）New eID 掛失及領、補、換發證作業流程及安全管制程序。

（四）New eID 全面換發作業（相片影像取像及規格、對象、申請書、通知單等）。

（五）戶政事務所收受及發放 New eID 作業流程。

（六）API 介接申請及應用管理。

（七）空白卡（含晶片）生產及運送安全控管。

（八）資安及作業流程管理規則（製卡中心端、卡片端、應用端）。

十一、研析委外服務方式

綜合研析上述第一至七項工作項目，進行統包（由單一廠商承作）或分項建置（製卡中心、API 應用服務中心及自然人憑證中心分開建置）委外服務方式之優缺點評析，並提供前述兩種委外服務方式之規劃報告書（分項建置委外服務應配合內政部政策進行規劃）。

第貳章、專案執行過程

壹、訪談與研析

一、卡片(含晶片)及其製發管理等相關議題研析

為規劃符合 New eID 產能之設備、數量、成本分析，本團隊訪談現行與製卡相關之廠商，蒐集現行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，以供本案規劃研析之用。

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

二、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，本案規劃開發 New eID 管理系統，作為 New eID 管理中心，整體系統設計須與相關系統（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，並須包含 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、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，本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，以納入本案系統建置之規劃建議。

表 2：系統建置相關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

貳、規劃報告交付時點與進度整體說明

一、交付時點

（一）於 108 年 7 月 10 日交付以下報告：

1. 「卡片（含晶片）規格及需求規劃」、「製卡中心規格、管理規範及安全規劃」、「製發管理規劃」、「自然人憑證規劃」、「新身分證應用軟體規劃報告書」、「新身分證晶片內容遠端更新規劃報告書」、「API 應用程式規劃報告書」。

2. 另依於 108 年 8 月 23 日召開審查會議決議，將「新身分證應用軟體規劃報告書」、「新身分證晶片內容遠端更新規劃報告書」、「API 應用程式規劃報告書」併寫成「API 應用程式整體規劃建議報告書」。

（二）於 108 年 8 月 10 日交付以下報告：

1. 「各項標準作業程序（SOP）」（New eID 印製及品質控管、New eID 空白卡及製發安全控管、New eID 掛失及領、補、換發證作業流程及安全管制程序、New eID 全面換發作業、戶政事務所收受及發放新身分證作業流程、API 介接申請及應用管理、空白卡（含晶片）生產及運送安全控管、資安及作業流程管理規則）、

「先期作業期間 eID 宣導資料」、「建置及換發期間 eID 專屬網站、宣導資料及戶所人員教 育訓練課程規劃報告書」。

2. 續依內政部需求將「New eID 掛失及領、補、換發證作業流程及安全管制程序」、「New eID 全面換發作業」、「戶政事務所收受及發放新身分證作業流程」整併成「各項標準作業程序（SOP）New eID 全面換發作業規劃報告書」。

（三）108 年 9 月 10 日交付以下報告：

「研析委外服務方式規劃報告」及「新一代國民身分證換發系統建置及維護案建議書徵求文件」。

二、進度整體說明

本團隊依約交付上開報告後，內政部即邀請專家學者召開審查會議，期間本團隊持續就內政部戶政司、資訊中心、移民署、警政署，以及行政院資通安全處、國家發展委員會、外交部、金融監督管理委員會、交通部、主計總處、財政部、法務部、法務部調查局、各直轄市、縣(市)政府等機關提供與本案相關之意見進行研議、溝通與討論，本團隊蒐集前開機關與審查委員意見後，按需求意見分析評估，召開會議討論修正規劃方向與內容後，嗣依據內政部與外部審查委員意見滾動修正，並於 108 年 12 月 13 日完成結案成果報告。

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

New eID 依據卡面之規劃原則設計卡面記載項目，本報告提供 New eID 卡面欄位內容，及卡面欄位名稱規劃建議。

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，以及主張簡約設計等原則，將配偶、父母姓名等個人隱私資料存放於晶片內，另以簡約為基礎的設計元素，將卡片正面之記載欄位作精簡設計，僅保留具有個人識別功能之欄位，諸如「姓名」、「統一編號」、「出生年月日」及「相片」等。

2. 中英對照原則

鑒於行政院業於 107 年 12 月 6 日確定「2030 雙語國家政策發展藍圖」之方向，建議卡面記載項目（包含欄位名稱及欄位內容）皆以中、英雙語並列為之，以達到雙語國家政策之落實。

此外，《國籍法》業於 105 年修正，關於「歸化」之規定已大幅放寬，是以，New eID 之服務對象將觸及更多母語非中文之人士，卡面記載項目調整為中、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下表 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，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) 記載當事人婚姻狀態為「有」、「無」，顯示欄位名稱「結婚狀態」。另如採取配合雙語國家政策之調整，英文則記載「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，是以，爰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」，係自製證日期起算，滿 5 年或 10 年為「應換領日期」，並以 14 歲作為分界，未滿 14 歲，應換領日期定為 5 年，14 歲以上未滿 65 歲應換領日期定為 10 年，65 歲以上無應換領日期。

(4) 列印證件號碼條碼，條碼下方顯示證件號碼，但不標註欄位名稱「證件號碼條碼」，將每張卡片出廠配號之卡號作為證件號碼。

(5) 列印國民身分證統一編號條碼，但不標註欄位名稱「國民身分證統一編號條碼」，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」，建議第一排內容為證件類別、國籍、證件號碼及統一編號；第二排內容為出生日期、性別、應換領日期及國籍；以及第三排內容外文姓名。

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。
證件號碼		背面	欄位名稱「證件號碼」無庸顯示，欄位內容應顯示「欄位條碼」下方。
國民身分證統一編號條碼		背面	欄位名稱「國民身分證統一編號條碼」無庸顯示，欄位內容不顯示「欄位條碼」下方。
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

本次建議規劃之 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，並循 94 年版之身分證，循例放置國旗。

另外在卡面字型選擇上，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宋體。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（含卡片耐用性、抗彎曲、耐磨、防水、抗污、耐高溫等規格）

(一) 卡片材質

依照規劃原則，空白卡片將採用 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（含晶片存取設計）

(一) ISO / IEC 相關標準：

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

(二) ICAO Doc. 9303

(三) 晶片通訊協定：

本晶片規劃設計，需符合雙介面的資料存取方式，藉由標準 ICAO 讀卡機、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：

3. 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。

4. 非接觸式介面：需符合 ISO/IEC 14443 Part 2，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。

(四) 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。

(五) 非接觸式介面感應距離只能在數釐米內。

(六) 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. SHA 安全雜湊演算法（Secure Hash Algorithm），需支援 SHA_224，SHA_256，SHA_384，SHA_512。
8. 卡片內金鑰產製（on card key pair generation），私鑰（private key）不可匯出。

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

(八) 硬體驗證需通過安全認證 Common Criteria EAL 5+（含）以上。

(九) 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。

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

(十一) 使用年限至少十年。

五、晶片記載項目的作業規範

參照國際民航組織（ICAO）之電子防偽機制及存取控制機制，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」及「ICAO 區」等 5 區。各區語言之使用原則，ICAO 區根據 ICAO 9303，此區全部以英文記載。非 ICAO 等 4 區，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。

主要區域規劃使用需參照下列方式：

(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，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. 資料異動方式：戶籍地址（僅到村里鄰）欄位為可以異動的欄位資料，民眾需持卡至戶政機關進行更新。
4. 資料顯示方式：以村里鄰代碼及中英文表示，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之問題及創造便利性。

5. 資料格式規範：本區資料格式規範參照 ICAO 規範。

(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」、「證件號碼」、「應換領日期」及「製證日期」共計 9 項。前揭「戶籍地址」須記載完整戶籍地址。

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，即身分證統一編號後 6 碼）或 MRZ 機讀碼才可讀取。

3. 資料異動方式：公開區中之資料，「役別」、「戶籍地址」欄位，民眾可持卡至戶政機關進行更新。其餘欄位為唯讀欄位，不可異動。

4. 資料顯示方式：以雙語（即中英對照）記載，為落實雙語國家之政策，爰建議部分欄位以雙語記載，建議欄位包括「姓名」、「戶籍地址」、「役別」、「結婚狀態」;「出生日期」、「應換領日期」及「製證日期」建議皆使用民國及西元紀年。

5. 資料格式規範：本區資料格式規範參照 ICAO 規範。

(三) 加密區

1. 資料內容：

「配偶姓名」、「父姓名」、「母姓名」、「出生地」、「性別」、「相片」、及「CAN」（供調閱公開區資料使用）共計 7 項。

2. 資料讀取方式：

晶片內密碼驗證方式：晶片內密碼驗證做法可參照歐盟公民卡規範 IAS-ECC 或 PKI 密碼驗證等同的機制；以用戶代碼設定密碼(PIN1)驗證成功後，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。

(四) 自然人憑證區

1. 使用方式：

用戶代碼預設初始密碼為亂碼，於領證時登載於「領證確認書」提供予民眾，建議民眾先更改預設之用戶代碼，重新設定為英數字 6-10 碼，並用修改後之用戶代碼，設定自然人憑證密碼才可使用（6-12 碼數字 PIN Code，下稱 PIN2），可作為簽章及身分認證使用，民眾可用一般晶片讀卡設備變更設定新密碼，驗證密碼成功後，便可使用自然人憑證，本區需參照 PKI 規範。

2. 規劃內容：

(7) 規劃至少可產製四組非對稱式金鑰對（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。

(8) 至少可存放六組憑證，並可設定憑證存取權限，需驗過 PIN2 碼後，可使用加密或驗證簽章，憑證寫入權限由發行者控管，發行者於本區係指自然人憑證中心。

(9) 卡片發行時包含根憑證、中繼憑證、二組金鑰對（RSA）之憑證，共四組憑證。另外二組（ECC）保留空間供未來可簽發憑證作為彈性使用。

(10) 安全驗證文件：

需提供五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：

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

B. 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。

C. 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。

(五) 新闢 ICAO 區調整方案

本報告建議於晶片中新闢 ICAO 區，該區內容完全遵循 ICAO 9303 規範，相關說明如下：

1. 資料內容：

配合 ICAO9303 規範，ICAO 區欄位包含發行國家、證件類別、外文姓名、證件號碼、國民身分證統一編號、出生日期、出生地、性別、應換領日期、製證日期、憑證、機讀碼、相片。

2. ICAO 9303 並未要求「出生地」、「性別」欄位之內容為應記載，而係由發卡國家（State）或組織（Organization）自行決定是否記載，準此，本報告分別評估如下：

(1) 出生地：

持有 New eID 者多為臺灣、澎湖、金門、馬祖出生之民眾，因出生地不具有身分識別功能，基於隱私最小揭露之考量，爰建議政策上可決定不予記載此一欄位。

(2) 性別：

雖 New eID 卡面上並未記載性別，考量國內自動通關所需，建議 ICAO 區記載具有身分識別功能之「性別」欄位，且機讀碼 MRZ 亦將列印性別，依據 ICAO 規範，男性以「M」、女性以「F」作為代碼，另基於 MRZ 對於性別隱私之保護，如不願對外揭露，可以列印「X」，表示性別未記載或不願公開，

因此與加密區性別保護之隱私要求並未衝突，ICAO 區之機讀碼設計僅為臨櫃使用，民眾有權利決定是否將卡片提出而保護隱私。至於非臨櫃使用，則必須透過加密區始得揭露性別，仍屬隱私保護措施。

3. 資料讀取方式：需符合 ICAO SAC（Supplemental Access Control）驗證，輸入機讀碼（MRZ）才可讀取，本區參照 ICAO 規範。

4. 資料異動方式：欄位均為唯讀欄位，只能讀取，不能複製或存取，不可異動。

5. 資料顯示方式：均以英文表示。

6. 資料格式規範：本區資料格式規範參照 ICAO 規範。

(六) 晶片各區資訊變動以及資訊變動辦理方式整理於下表。

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	唯讀，民眾不得持卡至戶政機關更新。
	外文姓名	
	統一編號	
	出生日期	
	結婚狀態	
	證件號碼	
	應換領日期	
	製證日期	
	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

晶片各區及其資料		不更換卡片情況下變更資料之方式
		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。
	相片	
	CAN	
自然人憑證區	姓名	各欄位均不可異動。
	身分證後 4 碼	
	憑證序號（證件號碼）	
	憑證有效日期	於展期情況下可異動。
ICAO 區	發行國家	各欄位均不可異動。
	證件類別	
	外文姓名	
	證件號碼	
	國民身分證統一編號	
	出生日期	
	性別	
	應換領日期	
	製證日期	
	憑證	
	機讀碼	
	相片	

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，更應強調以晶片方式作業的資訊防偽，特殊的差異有別於過往紙本型態。為此，結合資訊防偽之整體設計如下說明：

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項重複。

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（7 項）

（一）證件號碼：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，僅作為生產履歷管控之用。

（三）公開區讀取碼：與公開區相應之個人化讀取碼。

（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，寫入後即無從修改，例如 ICAO 區。

（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。

參、卡片（含晶片）安全防護措施

一、晶片安全規範與規格

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) 被動認證（Passive Authentication，PA）。

(三) 主動驗證（Active Authentication，AA）。

(四) 晶片驗證（Chip Authentication，CA）。

(五) 終端驗證（Terminal Authentication，TA）。

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

(七) 密碼管理（PIN Management）。

(八) 金鑰管理（Key Management）。

(九) 安全通道（Secure Channel）。

(十) 存取條件（Access Condition）（如表 5）。

(十一) 資料簽章。

表 5：卡片存取權限

卡片應用類別	最低存取權限
ICAO 區	機讀碼 MRZ
戶籍地區	無
公開區	安全通道+機讀碼 MRZ 或讀取碼 CAN
加密區	安全通道+ PIN1 碼+ 檢核機關合法授權憑證（EAC） （本區各欄位需為獨立授權，檢核機關可分欄位提供資料）
憑證區簽章及加密金鑰使用	安全通道+ PIN2 碼

肆、臨櫃取像規格及方式

一、規劃作法

因 New eID 規劃須符合 ICAO 規範，因此無論民眾繳交或上傳之數位相片，皆應符合 ICAO 9303 之要求，換言之，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，建議參考依據《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，因此，本報告謹彙整如下表，並以接近或符合 ICAO 9303 之方向提出建議：

表 6：New eID 相片規格修正建議[1]

項目	現行紙本國民身分證	ICAO 9303、晶片護照	New eID 建議
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。	考量未來自動通關使用，New eID 採用相片之拍攝時間為六個月內
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。

[1] https：//en.wikipedia.org/wiki/National_identity_cards_in_the_European_Economic_Area（最後瀏覽日期：2019 年 7 月 1 日）。

項目	現行紙本國民身分證	ICAO 9303、晶片護照	New eID 建議
繳交列印相紙	以高解析度沖(列)印在高品質相紙上。以數位相機拍攝之相片，必須為高彩度而且以相紙沖（列）印。	如相片是以數位相機拍攝，相機必須具備至少 300 萬像素（pixels）功能且設定為「最高品質、高彩度」,並以高品質光面相紙沖(列)印。倘提供之相片列印品質不佳或相紙過薄，以致無法製作,將不予採用。	電子檔規格限定 JPG 格式，檔案大小至少 600 DPI 以上,至少需達 1,062 像素，寬度至少需達 826 像素。
繳交數位相片	當事人如係繳交數位相片，其規格除須符合上揭規定外，其相片影像電子檔規格限定 JPG 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。	（尚未開放上傳數位相片）。	電子檔規格限定 JPG 格式，檔案大小不得大於 5MB ，600 DPI 以上,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	倘所繳相片不符前述規定或經內政部掃描器處理後影像品質未達標準，應請 New eID 申請人重新繳交數位相片。 倘因民眾修圖導致領證時無法辨識人貌，應重新申請。

項目	現行紙本國民身分證	ICAO 9303、晶片護照	New eID 建議
		繳交或郵寄至特定地址。	

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。」，附件內容如下：

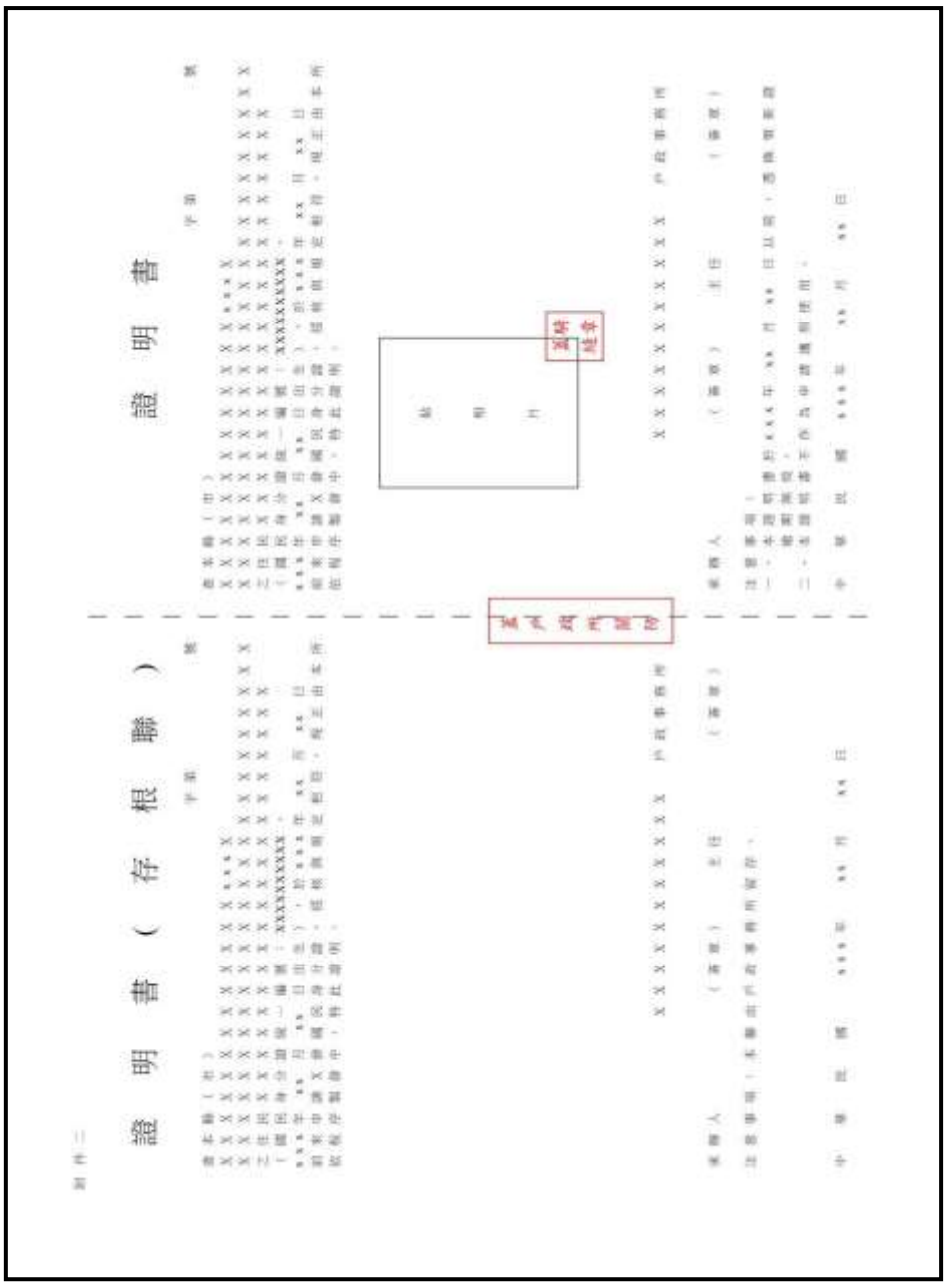
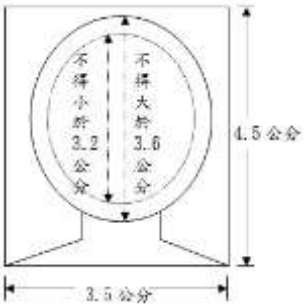


圖 1：舊版臨時證明書示意圖

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，因而提供新版之臨時證明書，其大小為 A4 型式，其樣式如下圖：

臨時證明書

<table>
<tr><td>姓名</td><td colspan="3"></td><td rowspan="4"> 

相片由系統直接列印。</td></tr>
<tr><td>出生日期</td><td>年　月　日</td><td>性別</td><td></td></tr>
<tr><td>國民身分證統一編號</td><td colspan="3"></td></tr>
<tr><td>國民身分證統一編號條碼</td><td colspan="3"></td></tr>
<tr><td>戶籍地址</td><td colspan="4"></td></tr>
<tr><td>申請時間</td><td colspan="4">年　月　日</td></tr>
<tr><td>使用效期</td><td colspan="4">年　月　日</td></tr>
<tr><td colspan="5">注意事項：
(一)本臨時證明書申請人，申請國民身分證，經核與規定相符，現刻正由本所依程序辦理中，特此證明。
(二)請以本證明書親自臨櫃換領新證。
(三)本證明書於領取新證後失其效力，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。</td></tr>
</table>

圖 2：臨時證明書示意圖

臨時證明書之申請，乃係因申請至領取 New eID 之期間，尚有使用身分證明文件之需求,由戶政事務所依程序核發;製證費用目前規劃不收取，惟若須收取工本費用，建議由臨時證明書之持有人繳交 20 元之規費。

臨時證明書之用紙採防偽材質，以增加其保護性及身分認證之功能。

內容須包含姓名、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、使用效期以及相片。其中，相片得由戶政事務所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；提供 QR Code 予民眾，以便隨時查詢身分證換補發狀態；另提供驗證序號，以便隨時查詢臨時證明書真偽。

臨時證明書得以作為身分證明之用，並設有使用效期。民眾須以臨時證明書親自臨櫃換領新證。本臨時證明書逾期無效，不得作任何其他用途。

一、規劃作法

本案建議除以紙本臨時證明書之方式辦理外，另可選擇無紙化行動臨時身分證 APP 作為臨時證明書之替代使用方式。

(一) 子法修法作業

因 New eID 之製發必然無法如同現行紙本國民身分證當場製發,建議《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 條應配合附件新格式之修正,並將行動臨時身分證 APP 納入修改作業。

(二) 行動臨時身分證 APP

為促進身分辨識之便利性，原已開通行動身分證服務之民

眾於提出 New eID 掛失後，行動身分證 APP 之功能應立即失效。如民眾申請行動臨時身分證服務，臨櫃取得戶政事務所授權後，透過驗證方式下載行動臨時身分證 APP，此行動臨時身分證條碼僅提供個人資料授權功能及代碼化技術（動態條碼產生功能）用以驗證身分，不提供行動自然人憑證簽章功能，再次領取新 New eID 後，行動臨時身分證立即失效，下圖說明其適用方式。

圖 3：行動臨時身分證 APP 使用示意圖

二、全面換發時期之因應

(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，申請換領 New eID 時並無收回舊證，均領取 New eID 時，才會回收現行紙本身分證，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換發 New eID 者

現行紙本身分證遺失之民眾，於全面換發期間僅能透過臨櫃方式申請換發 New eID，則應於其申請時發給臨時證明書。

若民眾以現行紙本國民身分證申請換發 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，由於製卡階段至領卡階段尚有時間差，倘其有身分辨識之需求，亦應於掛失原紙本國民身分證後，再至戶政事務所申請臨時證明書。

三、已完成 New eID 之換發者

民眾一旦完成 New eID 之換發後，倘有遺失、申請戶籍登記導致卡面資料異動，或申請更換相片等情形，而申請補證或換證時，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、當晶片失效時卡片是否有效之評估

New eID 除可以晶片進行身分識別，其卡片實體本身亦具有身分辨識功能，因此，晶片失效時，卡片外觀尚無從得知。「僅使用卡面資訊之情境」，卡片自得認為尚屬有效；以現行 IC 健保卡為例，於金融機構 KYC 實務經常作為身分辨識使用（即俗稱「雙證件」），晶片縱因物理磨損、接觸不良等因素而無法使用，卡片本身仍不失身分辨識功能。

「須使用晶片資訊之情境」，卡片自無從認尚屬有效；以現行 IC 健保卡為例，晶片因物理磨損、接觸不良等因素而無法使用，醫療院所即無從讀取晶片資訊，通常僅先以卡面資訊進行身分識別，並尋找病歷，掛號或批價時則請民眾押金，以未攜帶卡片之方式處理，

並請民眾儘速換卡俾於時間內退還押金。

據此，晶片失效僅無法提供數位資料及簽章，但卡片應換領日期之內，若無更換新卡，其仍可以作為身分識別之用。

柒、卡片與憑證之效期運用

一、效期說明

New eID 不訂定效期，但卡面記載「應換領日期」，於一般情況下，應換領日期為 10 年，惟基於密碼技術發展以及資訊安全考量，憑證效期為 5 年，屆期時可再進行憑證展期作業，延展一次 5 年之效期，故憑證之效期共 10 年，藉以得配合 New eID 之 10 年之應換領日期。

二、規劃作法

(一) 原則說明

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。

倘 New eID 卡片金鑰載具的效期設定為 10 年時，則憑證的效期為 5 年，憑證屆期時可再進行憑證展期作業，展期後之憑證效期最多可展延為 5 年，但不得超過該 New eID 卡片金鑰載具的效期，年限總計 10 年，且憑證展期作業僅適用於未被廢止之憑證。

民眾是在 New eID 發放時選擇暫停憑證使用時，則憑證效期與卡片效期相同，亦即憑證效期不得超過卡片金鑰載具效期，恢復使用期間亦須配合卡片金鑰載具效期。

(二) 卡片與憑證效期之運用情況

1. 憑證效期之計算

民眾取得製證日期為 110 年 7 月 1 日之卡片，應換領日期應為 120 年 6 月 30 日，則第一段憑證之效期應至 115 年 6 月 30 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 6 月 30 日，換言之，第二段憑證效期可能少於五年，惟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

(1) 14 歲以下民眾

其自然人憑證使用效期同卡片規範為 5 年且不得展期。

(2) 14 歲以上、65 歲以下民眾

其自然人憑證效期為 5 年，配合卡片 10 年效期，憑證屆期時可再進行憑證展期作業，最多可展延為 5 年。

(3) 65 歲以上民眾

其 New eID 卡片效期得設為超過 10 年或永久有效。對於此類 New eID 卡片金鑰載具效期超過 10 年的情況，其憑證在展延為 10 年且到期後將不得再次進行展期作業。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

為確保此卡片製發場所及作業安全，針對製卡中心規格、管理規範及安全規劃，內容包括：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。

本規劃係針對製卡中心規格、管理規範及安全規劃等面向提出原創性規劃建議，實際狀況應由建置廠商視具體情況及實務需求進行調整。

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。而製卡中心空間規劃除了要能符合內政部全面換發作業集中製卡產能所需，空間及規格應能達到每日最少產能 45,000 張卡片之要求，實體空間安全設計也要需考量消防、空調、不斷電、門禁及監控系統等實體機房安全，規劃內容如下圖所示：

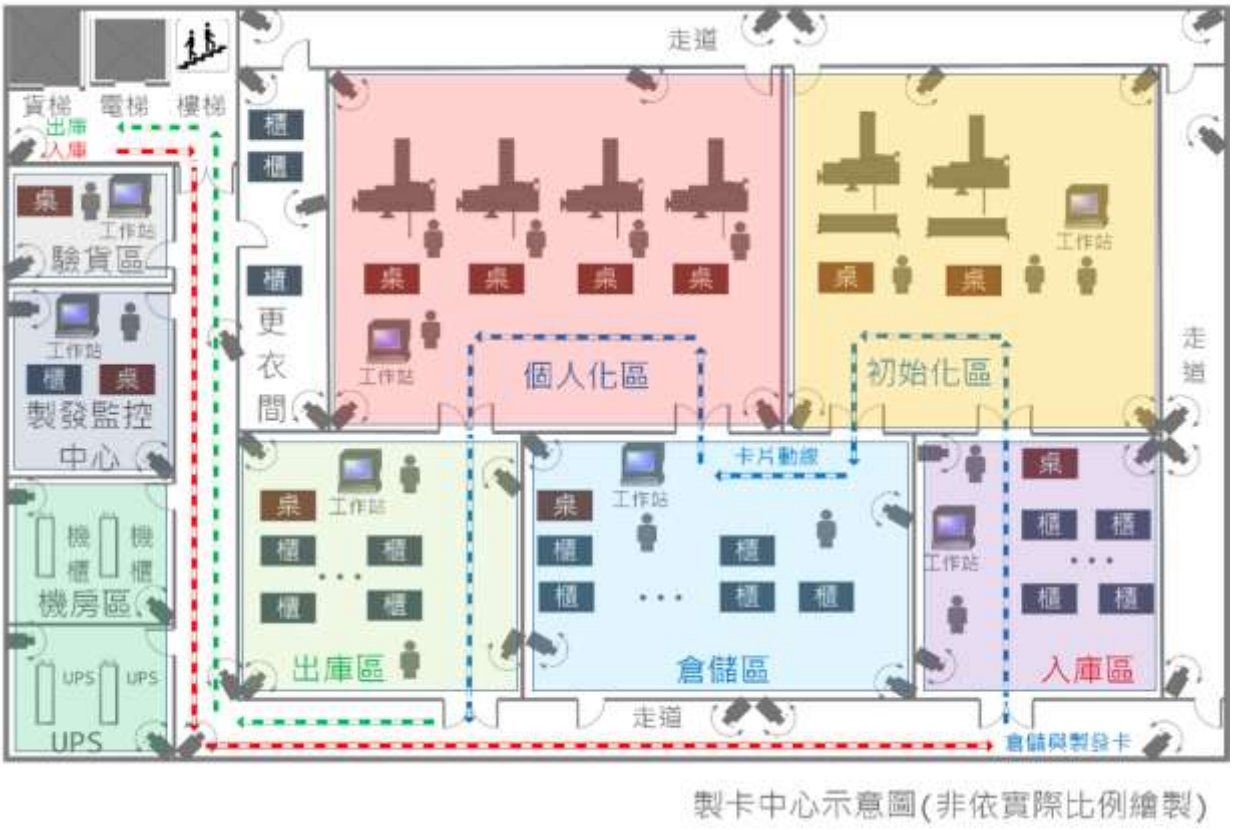


圖 4：製卡中心示意圖

(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（出庫區/倉儲區/入庫區）

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，庫房應至少有可庫存300萬張卡片之空間。

2. 入庫區存放空白晶片卡及安全耗材，出庫區存放製作完成之New eID、壞卡及廢卡。

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，建議應採實體區隔，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。

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，在非作業時間發現有人員（移動），則產生警報，現場音警報產生，且警報信號直接送到警局或外部保全公司。

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，即時通知機房管理人員。

(五) 機房區

提供製卡中心運作時其系統主機所放置的空間，此空間須設置機櫃以存放伺服主機以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. 內部皆有FM-200環保藥劑氣體滅火及自動排煙系統。

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. 大樓出入口設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，須事先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，即時通知機房管理人員，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紀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內政部全面換發作業計畫所需，目前規劃於 109 年 10 月至 112 年 3 月完成全國約 2,359 萬張身分證的換發作業，內政部可依實際進度動態調整。

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。

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紀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，提出如何進行災害應變之方案。

肆、建置與設備交付時程與數量評估

製卡中心最晚須於發卡前三個月完成實體機房的土木、隔間、門禁、空調、監控、消防與機電等基礎建置，並於發卡前一個月內完成相關發卡資訊設備與製發卡設備的安裝與測試。

伍、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，爰製卡中心收到一批定量的空白卡片後，須進行數量查核管控，入庫空白卡的總數量，須與交給戶政事務所的成品卡及製卡過程中損毀的卡片數量總合相符合。

製卡中心為達高強度的安全標準，相關設計應依據國際標準 EMV、PCI-DSS、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。

陸、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

為能進行相關管理，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、資料外洩應變計畫。

柒、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,各項系統並須自動紀錄相關人員所有之登錄/登出紀錄及執行工作內容。資料處理紀錄日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認證後始可啟動。

九、HSM 須具備金鑰分持機制。

十、建置廠商需依照上述面向提出相關規劃報告。

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

本規劃係針對製卡中心規格、管理規範及安全規劃等面向提出原創性規劃建議，實際狀況應由建置廠商視具體情況及實務需求進行調整。

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，採購之卡廠須取得 EMV（Europay, Mastercard, and Visa）或 PCI-DSS（Payment Card Industry Data Security Standard）或其他相同等級之規範之驗證，以確保空白卡產製及運送之安全性。採購之空白晶片卡規格應符合「卡片（含晶片）規格及需求規劃報告書」訂定之規格，並依規定印製卡面防偽措施，且晶片內容須已完成以下步驟：

1. 預先載入卡片上會使用到的相關 New eID 應用程式，即包含 ICAO、PKI 及其他應用於本案五區（即「戶籍地區」、「公開區」、「加密區」、「自然人憑證區」及「ICAO 區」）資料使用的相關卡片應用程式。

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，如卡片護膜、卡機色帶。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（卡片製發資料接受與卡片配對）。

(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五區資料空間。

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生產耗材（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、卡廠遞送庫房管理-空白卡入庫管理

二、初始化空白卡之庫房管理流程

(一) 空白卡出庫

(二) 初始化後半成卡入庫

三、製卡庫房管理流程

(一) 製卡領取半成卡（已初始化的卡片）

(二) 製卡後成卡入庫

四、壞卡之庫房管理流程

(一) 壞卡檢測完成入庫

(二) 壞卡銷毀

五、報廢卡之庫房管理流程

(一) 報廢卡檢測完成入庫

(二) 報廢卡銷毀

六、耗材庫房管理

當生產管理系統發現耗材庫存低於水位時，需透過生產管理系統進行耗材申請流程，填寫申請人員、申請理由、申請日期、申請地點、耗材申請數量等資訊於耗材申請單上送至對應耗材廠，等待耗材廠接收需求後將耗材裝箱編號送至庫房繳交。

七、成卡庫房管理

(一) 成卡入庫

(二) 成卡出庫

八、庫房檢核管理

(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相關卡片耗材，並淨空製卡機房。

(二) 庫房每月檢核

每月盤點作業於月底作業，於系統停止作業時確認及清點相關卡片耗材，並淨空製卡機房。

參、產品封裝檢測

New eID 製發完成在郵封前，須透過卡機終端進行卡片品質檢測，以卡機 QA 模組比對卡面印製資料之正確性，且卡片與卡機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。通過檢測後之 New eID 再以郵封機封裝。

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、空白卡運送方式

空白卡運送包裝均需有獨立之溯源碼，並提供運送清單（包含卡片類型、數量、作業編號、發貨日期、收貨日期及接受人員名稱與簽名），全程與相關系統連結。安全運送方式可利用：車輛運送、飛機運送或船舶運送。

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之溯源碼及運送編號(條碼)作為安全追蹤機制碼，並提供運送清單(包含卡片類型、數量、作業編號、發貨日期、收貨日期及接受人員名稱與簽名），建議每件封箱內卡片數量約 200 至 500 張，確保各戶所點收過程之正確性及便利性，另相關之安全機制需全程連結管理系統。

運送全程在溯源碼及運送編號（條碼）雙重控制下進行，運卡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。

有關運送頻率部份，建議直轄市採每星期運送 2 次，其餘各縣（市）採每星期運送 1 次，避免送達時間為下午時段或假日影響領取進度控管，採當日送達戶所，而離島縣市得視情況而定。

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，並持續維持其驗證有效性。

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。

(二) 進出人員管控

所有對外出入口（包括緊急出口）均應設有保全及警報、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，門禁系統紀錄所有進出狀況，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，自空白卡入庫後、製卡完成並運送後，控管卡片之狀態。

三、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：

(一) 評定安全影響範圍與召回成本，確認召回層級與範圍。

(二) New eID 管理系統列出擬召回之證件，確認召回數量。

(三) 確認召回晶片卡處理方式。

(四) New eID 管理系統廢止證件號碼對應之卡片，並提供 OCSP 及 CRL 名單進行查詢。

(五) 在 New eID 專屬網站公告，並通知需用機關加密區、公開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。

(六) 以簡訊、電子郵件或電話通知民眾持舊證申請換領新證。

(七) 戶政事務所受理民眾持舊證申請換發新證，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申請換證。

(八) 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。

(九) 戶政事務所需定時回報戶政司換證作業進度。

(十) 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。

(十一)保存相關召回紀錄以備日後查核之用。

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，且卡片與卡機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上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：

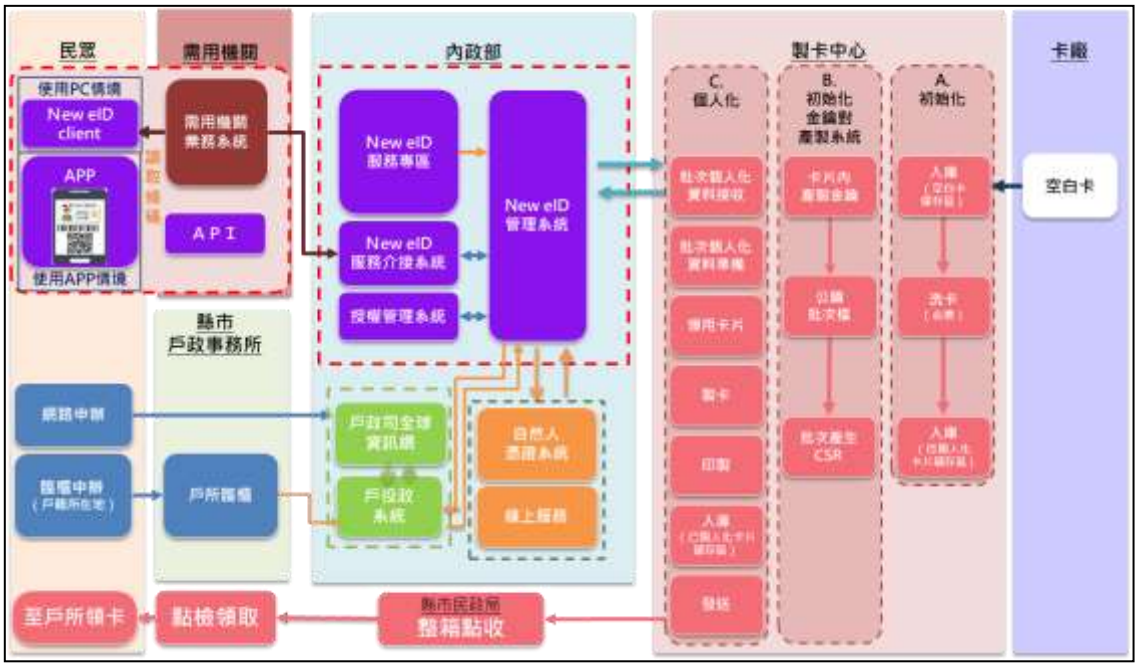


圖 5：系統架構與卡片製發管理整體架構圖

針對 API 應用程式、New eID 應用軟體及 New eID 晶片內容遠端更新作法之規劃，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）及Moblie APP 規劃。

New eID 服務介接系統關係可大致分為內部服務型 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：

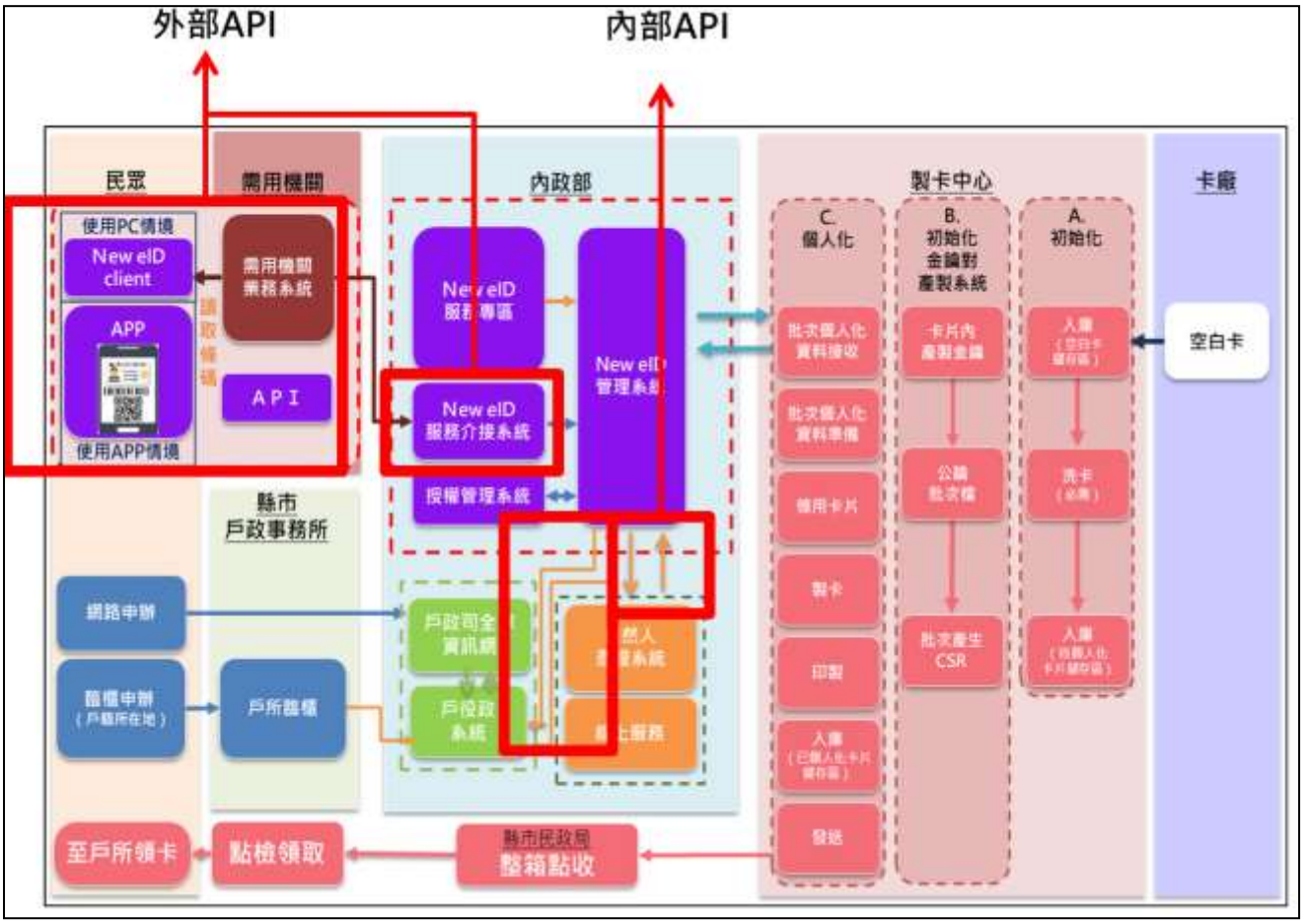


圖 6：New eID 服務介接系統關係圖

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）。

壹、New eID 相關應用情境說明

一、介接需求申請

申請 New eID 介接服務時，應填具介接申請書（如下表）並提交相關佐證資料送內政部辦理，申請完成後，申請人應先自行開發測試，待開發驗證完成後，方可進入正式環境執行。申請方式如下：

（一）線上申請：透過憑證（如工商憑證、組織憑證或政府機關憑證等）申請，且無需再將申請書及申請人身分證明等文件郵寄至內政部。

（二）書面申請：於線上填寫申請書印出後，檢附相關文件郵寄至內政部申請。

表 8：New eID 加密區 API 介接申請書範例

內政部戶政司「New eID 加密區 API 介接申請書」

				申請日期		
需用機關／單位申請資料	目的事業主管機關	中		機關代碼		
		英				
	需用機關單位名稱	中		統一編號		
		英		適用行業代碼		
	機關單位地址					
	申請目的					
	預計測試日期					
	主機網路位址			子網路遮罩		
	讀取權限	□配偶姓名 □父母姓名 □出生地 □性別 □相片 □CAN（供調閱公開區資料使用）				
	聯絡人		連絡電話		電子信箱	
	機關單位印信			機關單位負責人簽名		

受理機關審核資料（內政部戶政司）	審核意見	□提供 □無法提供	無法提供原因	□填寫資料錯漏 □主機網路位址不符 □數據線路編號有誤 □申請資料與業務性質不符 □其他：	
	預計測試日期	年 月 日		預計連結日期	年 月 日
	網路位址	申請機關通訊設備		安全閘道器	API Gateway 伺服器（SSL 連線通訊埠 443）
	子網路遮罩				
	承辦人（職章）		連絡電話		電子信箱
	科（組）長（職章）			單位主管（核章）	

二、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，需用機構可以直接下載 Open API 取得民眾同意後以接觸或非接觸方式使用讀取碼（CAN）讀取公開區資料，如姓名、國民身分證統一編號等，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，尚須取得內政部授權後，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。

內政部授權需用機關使用，每次使用均會檢核其授權狀態，但需用機關調用民眾個人之加密區資訊僅會紀錄於其應用系統，內政部並不紀錄民眾加密區讀取狀況，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、高科技園區為提供對象。由於此揭提供者不僅適用個人資料保護法且依據資通安全管理法納入資安稽核要求並有相關罰則，其內稽內控機

制強，此揭對象建議得申請 Seurce API。

2. 個人資料保護法之中央目的事業主管機關指定適用行業。個人資料保護法採取由各目的事業主管機關分散管理之模式，對於加密區資料之調閱，由該中央目的事業主管機關依據業務以及相關業務管理規範而指定該行業是否有其需要申請 Secure API。

三、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，將會要求民眾進行卡片密碼驗證輸入 PIN1，由 New eID 管理系統進行驗證完成之後，New eID 管理系統向戶役政資訊系統查詢最新資料後進行晶片資料更新。

（四）New eID 管理系統，將會註記本次更新紀錄。

（五）資料後續再透過 New eID 管理系統私鑰進行加密雜湊運算後傳遞至晶片，由晶片內之公鑰進行解密雜湊後比對 New eID 資料內容完成簽署，確認更新後之 New eID 之合法性與有效性。

四、個人端維護軟體功能情境與資安規劃

（一）資料檢視：

民眾輸入卡片密碼（PIN1）後可檢視晶片內之加

密區並利用晶片加密區之 CAN 欄位檢視晶片內之公開區資料。

（二）鎖卡解碼

1. 民眾輸入用戶使用者代碼，可進行鎖卡解碼。

2. 民眾領取 New eID 後使用個人端維護軟體，需輸入用戶代碼解鎖並設定新的晶片密碼（PIN1、PIN2）後方可使用 New eID，如忘記用戶代碼，則必須回到戶政事務所於 New eID 管理系統設定新的晶片密碼。

（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流程可能發生資安風險所採用之資安防護方法說明如下表 9。

表 9：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	• 唯一的對稱式及非對稱式金鑰 • 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 • 部份資料為唯讀，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	非授權讀取	• 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	非授權讀取 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
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

貳、New eID 基礎架構描述

在本節中，描述了 New eID 服務介接系統提供的服務以及對其操作環境的要求。此外，本節還介紹了 New eID 服務介接系統上下文中相關的所有其他模組及其共享的介面。

一、架構描述

（一）標準架構：需用機關 N_eID-Server 架構

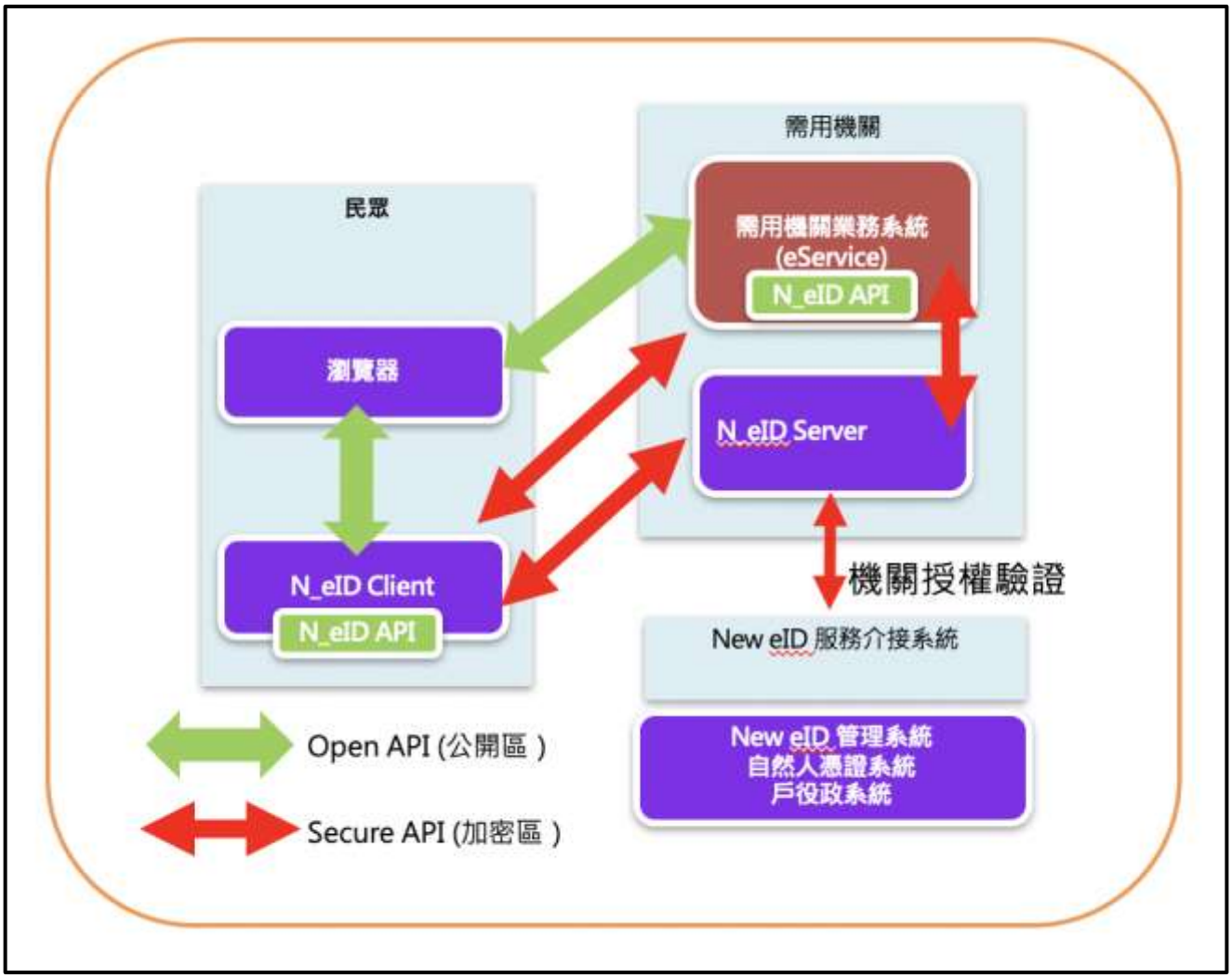


圖 7：標準需用機關系統規範架構

（二）以內政部自為需用機關建構 N_eID-Server

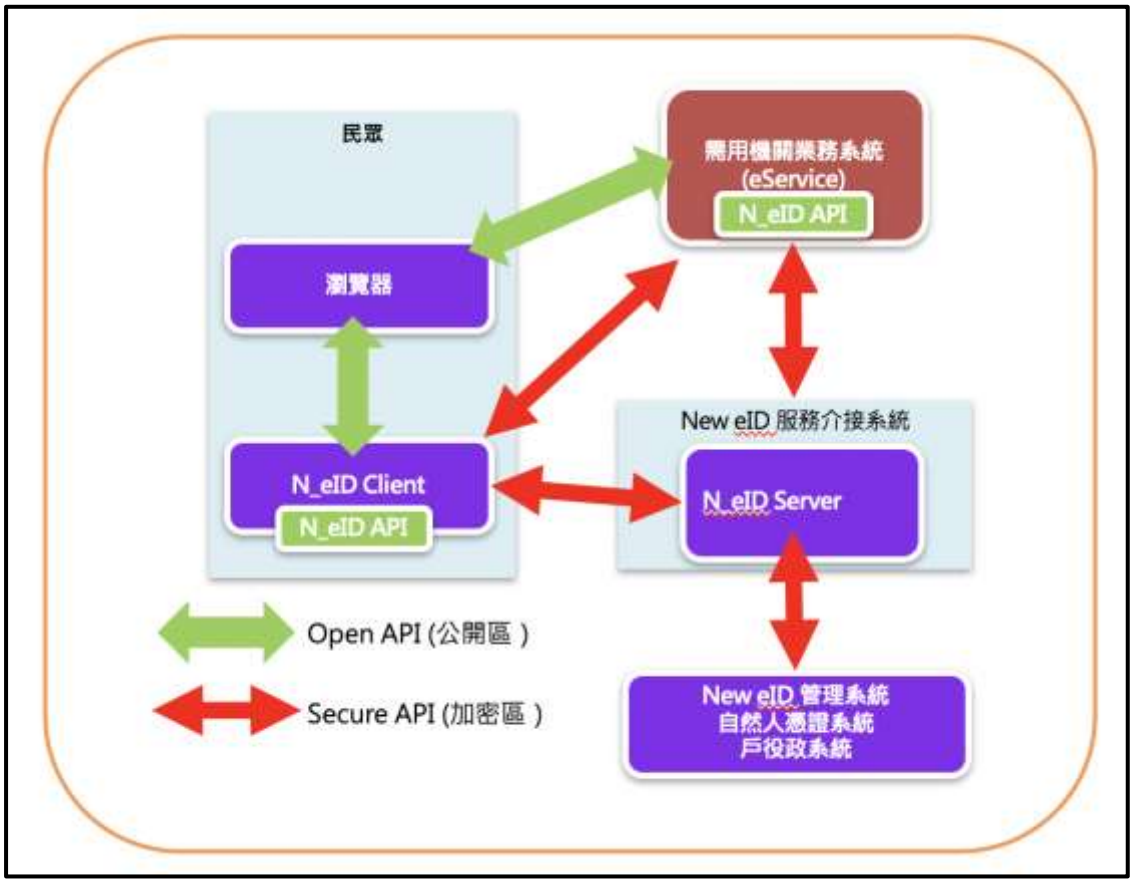


圖 8：內政部為需用機關架構描述

二、系統組成

N_eID Service 為 N_eID-Server 上之 WEB Service，可以作為單一伺服器運行。在這種情況下，必須滿足 TLS 安全通訊模型和 session 綁定的要求。N_eID-Server 必須執行身分有效性檢查，並提供所有其他強制性功能。

（一）需用機關業務系統（eService）

需用機關業務系統（以下簡稱 eService）實現民眾於瀏覽器中顯示的 Web 應用程式的應用邏輯。 本報告未限制 eService 提供的應用類型，可為各類政府機關與銀行單位等。在此上下文中，重要的是 eService

使用 N_eID-API 與 N_eID-Server 為其民眾提供相互線上身分驗證。 其意味著 eService 必須於加密區處理時實現基於 EAC 的線上驗證。eService 為每個線上認證接收或產生隨機預設共享金鑰（PSK）和 PSK 的唯一標示，以將 N_eID-API 和 New eID-Service 的 web session 綁定。N_eID_Server 為 N_eID Service 執行的每個線上身分驗證專門隨機產生 PSK。 eService 和 N_eID-Server 必須確保 PSK 的機密性，同時藉助 TCToken 將其轉移到 N_eID-Client。

（二）N_eID-Server

N_eID-Server 執行 N_eID-API 中加密區指定的伺服器端。為此，控制過程的應用程式邏輯和所有相關的安全算法應根據安全規範實現。N_eID-Server 為 eService 保存和管理認證憑證，並且必須保護 eService 的終端授權憑證不被濫用。要在 New eID 服務介接系統上提供服務，N_eID-Server 必須能夠存取下節所列出的所有介面。

（三）N_eID-Client

N_eID-Clinet 為一使用者使用之終端軟體，安裝於民眾電腦上，此 Client 整合Ｎ_eID-API 達成加密區與公開區與自然人憑證使用方式，此 N_eID-Client 亦可以依據業務不同的需求有不同的形式存在，欲設計的基本 N_eID-Client 使用原則為跨平台與支援目前市面上的瀏覽器呼叫。

三、系統介面

N_eID-Server 使用 N_eID-API 和公鑰基礎結構（PKI）與 N_eID-Client 通訊，利用在 New eID 服務介接系統的介面（如 SAML、SOAP、RESTful-Profile，實際介面依開發需求而定，本報告以 SAML 為例）上提供的服務。N_eID-Server 的介面設計需基於 Web Service 架構，因此可以透過開放網路進行 URL 定址。還可以透過可選介面提供 N_eID-Server 的附加服務。舉例來說，N_eID-Server 可以提供 eService 的身分證資料讀取權限。本報告描述的 N_eID-Server 或 SAML-Profile 之外的其他介面或內部介面不得用於交換民眾的個人資料。

（一）N_eID Interface

透過 New eID 服務介接系統（SOAP）中描述的 eID 介面，N_eID-Server 可以為 eService 提供一種使用 eID 功能進行線上驗證的簡便方法。替代方式為 N_eID-Server 可以提供 SAML-Profile 中指定的 SAML 處理或 RESTful 方式處理，本報告僅以 SOAP 與 SAML 為範例，RESTful API 其相關做法亦可按此架構建置。

（二）N_eID-API

本報告中指定的 N_eID-API 分為兩部分軟體組成：

1. Open API：

Open API 使用讀取公開區資料，有鑒於公開區資料使用 CAN 碼可直接讀取，故 eService 可直接使

用，N_eID-Client 亦可直接顯示公開區內容，但仍需要輸入 CAN 碼開啟讀取。

2. Secure API

Secure API 為加密區應用之 API，此 API 必須經由需用機關申請與審核後交付 eService 使用，由於讀取加密區需要使用者輸入 PIN1 碼並經過 N_eID-Server 做 EAC 認證，權限較高，當讀取加密區可取得 CAN 碼，即可透過 Open API 讀取公開區，故使用三方認證機制確保讀取之欄位合適且正確交付給需用機關 eService。

（三）Public Key Infrastructure

在本案中定義的 eID 功能的安全性基於公鑰基礎設施（PKI）的存在。與此 PKI 模組的連接允許 N_eID-Server 驗證是否從有效的 eID 接收資料，以及它允許 eID 驗證 eService 的真實性。因此，N_eID-Server 必須能夠存取公鑰目錄、憑證機構、不可信任名單和 CRL。 N_eID-Server 代表 eService 儲存終端授權憑證，並保護其免受濫用，符合授權管理策略。N_eID-Server 必須根據從授權管理系統請求 eService 的終端授權憑證。用於驗證 eID 有效性的 PKD 和包含 eID 的廢止清冊- 已撤銷的文件也必須由 N_eID-Server 從授權管理系統請求和接收。

四、eID 有效性驗證

N_eID-Server 必須檢查 eID 的有效性

（一）執行晶片驗證。

（二）執行被動身分驗證。

（三）檢查 New eID 或憑證狀態。

（四）檢查有效日期，另外使用提供的 CRL。

根據 eService 用於與 N_eID-Server 通訊的介面，N_eID-Server 必須根據錯誤代碼發送錯誤代碼。

參、New eID 基礎架構整合方式與流程說明

目前市場上針對 ID 認證架構有 SOAP、SAML、OAuth2 及 Open ID Connect，本報告提供 SOAP 與 SAML 整合案例來說明 New eID 整體架構，有鑒於歐盟大多數國家以 SAML 為主軸，SOAP 與 SAML 的 XML 加密機制嚴謹並比目前 Open ID Connect 架構來的相對安全，目前各國使用上與歐盟 eIDAS 運行多年已趨於穩定，且 New eID 加密區除了認證功能亦須考量授權架構，故針對本案公開區之 Open API、加密區之 Secure API（SOAP 與 SAML）提供使用情境與對應設計。

一、Open API 服務情境架構

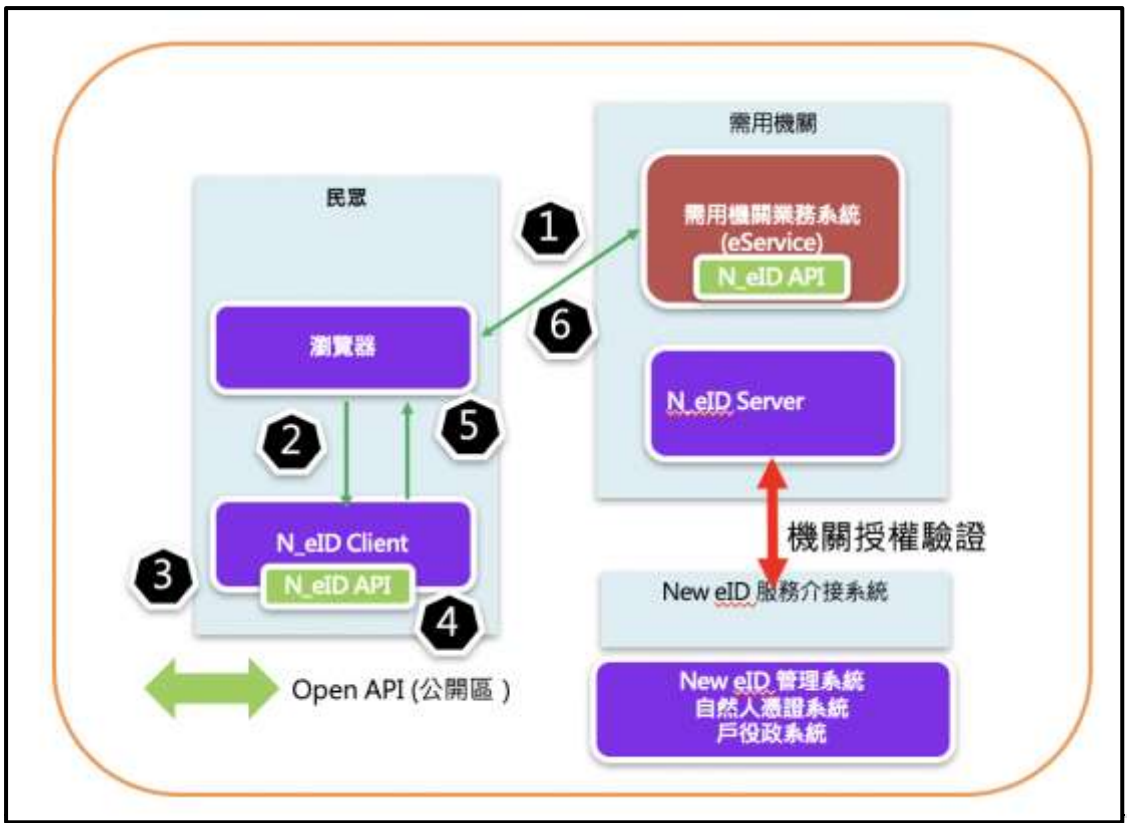


圖 9：Open API 服務情境

（一）民眾登入需用機關網站執行業務。

（二）需用機關依據申請業務需民眾提供 eID 身分驗證，即呼叫 N_eID_Client。

（三）New_eID_Client 啟動對話框說明此業務需民眾之公開區資料作身分驗證，民眾同意後即跳出輸入 CAN 碼對話框。

（四）民眾輸入 CAN 碼。

（五）New eID_Client 及提供公開區的資料欄位與簽章經由瀏覽器 TLS 傳輸至需用機關。

（六）需用機關收到資料後驗證其簽章是否為合法身分證資料。

二、Secure API 服務情境架構（SOAP）

New eID-Server 是參考 ISO/IEC 24727(Identification cards – Integrated circuit card programming interfaces）為基準，以 Web Service 描述語言（WSDL）或 RESTful 描述的 Web 服務。New eID 服務介接系統使用的數據類型，屬性和參數單獨描述為 XML 模式定義（XSD）或 json 結構。N_eID-Client 與 N_eID-Server 間之連結，包含如何在瀏覽器及 eService 間進行一個預先定義之連結來進行基於 EAC 之線上認證。

三、Secure API 服務情境架構（SAML）

SAML 中定義的安全標記語言是國際公認使用的身分認證標準。是一個基於 XML 的開源標準資料格式，它在當事方之間交換身分驗證和授權資料，尤其是在身分提供者（IdP）和服務提供者（SP）之間交換。在一般情形下，SAML 協議採用三方實體模型，並基於其中兩個身分提供者（Idp，也就是 N_eID-Server）和服務提供者（SP, eService）之間的信任關係。

使用 SAML 以使身分驗證協議的原則保持不變，並且可以實現安全，合法的身分驗證。其基礎是 eService 可以委託由第三方執行線上認證。New eID SAML 架構與 SAML 定應如下表：

表 10：New eID 與 SAML 角色對應

New eID 架構	SAML 標準定義	描述
User	User	民眾使用 Browser 和 N_eID-Client 在 eService 處進行聯繫和身分驗證，以及驗證 eService 的身分。
N_eID_Client	User Agent	N_eID-Client 提供民眾代理的功能，並引導民眾完成線上驗證過程。
eService	Service Provider（SP）	eService 也稱為應用方，並使用 eID 服務來驗證民眾的身分並驗證自己。
N_eID_Service	Identity Provider（IdP）	eID 服務代表 eService 執行線上身分驗證，並負責檢視 SP 權限。

四、New eID-Server（SOAP）

（一）功能清單

為描述 New eID 服務介接系統所提供的所有功能。從技術而言，此 Web 服務在相應的 WSDL-File 中進行了描述。

表 11：Web service API

N_eID-Server		
useID		
Input	parameters	useIDRequest
Output	parameters	useIDResponse
getServerInfo		
Input	parameters	getServerInfoRequest
Output	parameters	getServerInfoResponse
getResult		
Input	parameters	getResultRequest
Output	parameters	getResultResponse

1. useID

eService 必須使用函式 useID 來初始化新的線上驗證。

(1) Request

表 12：Function useID Request

F：useIDRequestType	
P：UseOperations	OperationRequestType
P：AgeVerificationRequest	AgeVerificationRequestType
P：PlaceVerificationRequest	PlaceVerificationRequestType
P：PSK	PreShareKeeeyType

eService 必須使用函式 useID 的使用來選擇 New N_eID-Server 並執行民眾端的 N_eID-Client 執行操作。這些操作包括讀出選定的資料組並執行年齡或地點驗證。useID 函式只能在每個 session 期間使用一次。獨立於其他操作，N_eID-Server 必須執行 eID 有效性檢查。函式的參數如上表所示：函式 useID Request 和下表：函式功能 useID 參數。

表 13：函式功能 useID 參數

參數名稱	**功能描述**
UseOperations	eService使用此參數來定義N_eID-Server嘗試從eID讀取的資料和功能
AgeVerificationRequest	執行年齡驗證請求時，此參數給出eID所有者應該完成年齡檢查。在UseOperations參數中請求AgeVerification時，必須存在此參數。如果eService請求，

	N_eID-Server必須使用此參數並執行年齡驗證。
PlaceVerificationRequest	執行場所驗證請求時，此參數可以驗證CommunityID。在UseOperations參數中請求PlaceVerification時，必須存在此參數。N_eID Server必須使用此參數來執行位置驗證。
PSK	如果N_eID-Server支援此功能，則eService可以使用此參數進行預設共享金鑰（PSK）的初始傳輸，然後N_eID-Server必須在useIDResponse中使用相同的PSK。

(2) Response

表 14：函式 useID 返回值

F：useIDResponseType	
P：Session	SessionType
P：eIDServerAddress	anyURI
P：PSK	PreSharedKeyType
P：Result	ResultType

對功能 useID 的回應顯示 N_eID-Server 的服務能夠打開所請求的線上身分驗證的 session。函式 useID Response 如上表所示。

N_eID-Server 允許每個 eService 的最大數量的同時活動 session。

建議為該最大值設置適當的值，以便多個數位服務的大量載入不會導致其他數位服務的可用性受限。如果超過一個 eService 的最大並發 session 數，則 New N_eID-Server 必須在 Result 參數中使

用 ResultMinor URI/useID＃tooManyOpenSessions 發送錯誤訊息。

表 15：Function useID Parameters

回應名稱	功能描述
Session	sessionID將useID函式使用與getResult函式使用連接起來，並且必須出現在此訊息中。它必須由N_eID-Server為每個特定的線上認證產生唯一值。
eIDServerAddress	使用此參數，N_eID Server可以通知eService有關目標地址的訊息，如果地址不是靜態的，則應該在該目標地址下聯繫N_eID-Server的N_eID_API模組。 eService必須將此目標地址準確放置在TCToken中的ServerAddress參數中。
PSK	PSK是N_eID-Client和N_eID-Server之間加密通道的初始密鑰，如表一所示：Webservice概述。eService必須將此PSK用於TCToken。如果在eService使用函式useID期間已經將PSK傳輸到N_eID-Server，則相同的PSK必須是N_eID-Server回應的一部分。如果此訊息中發送的PSK與請求中發送的PSK不同，則eService將中止線上認證。
Result	必須顯示是否可以處理請求或發生錯誤。

2. getResult

eService 必須使用函式 getResult 來為函式 useID 的使用請求結果。

(1) Request

表 16：Function getResult Request

F：getResultRequestType	
P：Session	SessionType
P：RequestCounter	Integer

一個線上身分驗證中可能多次使用 getResult 函式。eService 必須在 Online-Authentication 中使用該函式，直到它不再獲得 ... / getResult #noResultYet 錯誤。如果使用不包含.../getResult#noResultYet 錯誤的訊息回應函式 getResult 的請求，則 eService 不再使用該 Session。如果函式 useID 的使用和函式 getResult 的使用之間的時間超過 N_eID-Server 定義的時間限制，則 Session 也應該到期，具體取決於它的操作要求。

表 17：Function getResult Parameters

參數名稱	**功能描述**
Session	必須為此函式使用提供線上身分驗證的 Session ID。
RequestCounter	在線上身分驗證中進行功能使用的計數器必須是唯一可識別的。對於 Online-Authentication 中的每個 getResult 函式使用，此值必須遞增 1。 此過程可防止對 getResult 函式的重送攻擊。

(2) Response

表 18：Function getResult Response

F：getResultResponseType	
P：PersonalData	PersonalDataType
P：FulfillsAgeVerification	VerificationResultType
P：FulfillsPlaceVerifaction	VerificationResultType
P：OperationsAllowedByUser	OperationsResponderTypte
P：Result	ResultType

如果結果存在於 N_eID-Server，則函式 getResult 的回應為 eService 提供所請求的線上身分驗證的結果。執行該函式後沒有錯誤，Session 將會變為無效，N_eID-Server 必須刪除查詢的資料。如果 N_eID-Server 使用除了包含 noResutYet 錯誤之外的訊息來回答函式 getResult 的使用，則 Session（ID）必須設定無效並且 N_eID-Server 不再接受使用。如果函式 useID 的使用和函式 getResult 的使用之間的時間超過 N_eID-Server 定義的時間限制，則 session 也應該到期，具體取決於操作要求。

函式的返回值如上表 getResult 請求和下表 getResult 參數所示。

表 19：Function getResult Return Values

回應名稱	功能描述
Personal Data	如果成功處理線上身分驗證，則必須包含 N_eID -Server 從 eID 中讀取的資料。
FulfillsAgeVerification	如果執行年齡驗證，N_eID-Server 必須在函式 getResult 的回應中包含參數 FulfillsAgeVerification。 如果 eID 的所有者已達到要求的年齡，則該參數的值應為 true;如果 eID 的所有者尚未達到所要求的年齡，則該值應為 false。
FulfillsPlaceVerifaction	如果在 UseOperations 參數中啟用地點驗證並且函式使用成功，則地點驗證的結果必須包含在此返回值中。
OperationsAllowedByUser	定義在應用終端授權憑證和民眾同意之後可以從 eID 中有效讀取的資料和功能。 如果 N_eID-Server 成功處理線上身分驗證，則必須存在該參數。
Result	必須顯示是否可以處理請求或發生錯誤。 特別是，錯誤... / getResult #noResultYet 出現。

3. getServerInfo

函式 getServerInfo 必須向 eService 提供有關 N_eID-Server 的資料。eService 可以藉助此功能檢查 N_eID-Server 的設定。

(1) Request

函式的參數是 nullType 類型的參數。此類型根本不包含任何訊息，僅用於啟用正確使用函式。它可以隨時由 eService 使用。

(2) Response

表 20：Function getServerInfo Response

F：getResultResponseType	
P：ServerVersion	VersionType
P：DocumentVerifactionRight	OperationsSelectorType

表 21：Function getServerInfo Return Values

回應名稱	**功能描述**
ServerVersion	必須顯示 N_eID-Server 目前的 eID-Interface 的版本。
DocumentVerificationRights	必須顯示 eService 可能與目前對應的終端授權憑證一起使用的操作。

（二）安全措施

eID-Interface 為連接 eService 和 N_eID-Server 的通訊通道（SOAP）的介面。傳輸的加密和 XML 訊息的簽章用於保證傳輸的資料和函式使用的機密性、完整性和真實性。

1. Encryption

由於 eService 和 N_eID-Server 直接相互連接，並且通訊中不涉及第三實體，因此傳輸級別的加密就已足夠。如果 eService 和 N_eID-Server 通過其他開放網路（例如 Internet）進行通訊，則它們必須使用符合 TLS 的 TLS 1.2（含）以上的安全連接進行通訊。由於 eService 和 N_eID-Server 之間的信任關係，必須執行客戶端和伺服器身分驗證。 如果客戶端身分驗證失敗，則 N_eID-Server 必須拒絕連接。

2. Signature

eService 和 N_eID-Server 必須將 XML 簽章應用於使用 N_eID-Server 發送的所有 XML 訊息。因此，必須使 Web 服務指定的 InitiatorToken 和 RecipientToken。XML 簽章的要求。目前這意味著必須使用以下套件之一：

(1) Basic256Sha256

(2) Basic192Sha256

(3) Basic128Sha256

具有無效 XML 簽章的 N_eID-Server 接收的 XML 訊息必須僅使用錯誤代碼 ... / common # internalError 來回答。

InitiatorToken 是一個 X.509 憑證簽章，eService 必須使用該憑證簽章來簽署對 N _eID Server 中間通訊的的每個請求。N_eID-Server 應檢查簽章的有效性，並藉助其 X.509 憑證分成不同的客戶端。N_eID-Server 不得回答使用無效 X.509 憑證簽章或不簽章的請求。

RecipientTokeRecipientToken 是 X.509 憑證簽章，N_eID-Server 必須使用該憑證簽章來簽署使用 eID-Interface 發送到 eService 的每個回應。eService 應檢查簽章的有效性，並且不應處理使用無效的 X.509 憑證簽章或不簽章的資料。

3. Session Binding

eService 必須使用與 N_eID_Server 協商的 PSK

來創建 TC Token，session 綁定中描述執行通道綁定但不可直接影響 N_eID-Server 的其他措施。兩者都是執行將瀏覽器和 eService 之間的通道 TLS 綁定到 N_eID-Client 和 N_eID-Server 之間的 TLS 加密通道的最終目標所必須執行的。

eService 只接受並處理綁定到現有 Web Session 的 N_eID-Server 有效回應。N_eID-Server 只接受並處理來自授權數位服務的有效請求，並且必須確保只接受 N_eID-API 上的有效請求。為此目的，N_eID-Server 必須驗證 N_eID-Client 用於初始化 N_eID_API 通訊的 PSK，其每個 SessionIdentifier 與先前在 eID-Interface 上為一個特定 session 協商的 PSK ID 匹配，並且安全連接是可信的。

五、New eID-Server（SAML-Profile）

（一）基本要求

N_eID-Service 執行 SAML-Profile 的基礎必須是 SAML 預設文件。因為 eService 和 N_eID-Service 必須使用 SAML 中指定的傳輸機制來實現 HTTPS 重新轉址綁定。SAML 訊息必須在重新轉址的 Location 中進行 URL 編碼傳輸。

對於此預設文件的使用，必須按照本節所述使用 SAML 的協議，認證請求協議中指定的請求協議。下表顯示了 SAML 中定義的角色到此上下文中顯示的 New eID 架構角色的對應。

表 22：New eID 架構角色的對應

New eID 架構	SAML 標準定義	描述
User	User	民眾使用 Browser 和 N_eID-Client 在 eService 處進行聯繫和身分驗證，以及驗證 eService 的身分。
N_eID_Client	User Agent	N_eID-Client 提供民眾代理的功能，並引導民眾完成線上驗證過程。
eService	Service Provider（SP）	eService 也稱為應用方，並使用 eID 服務來驗證民眾的身分並驗證自己。
N_eID_Server	Identity Provider（IdP）	eID 服務代表 eService 執行線上身分驗證，並負責檢視 SP 權限。

（二）安全措施

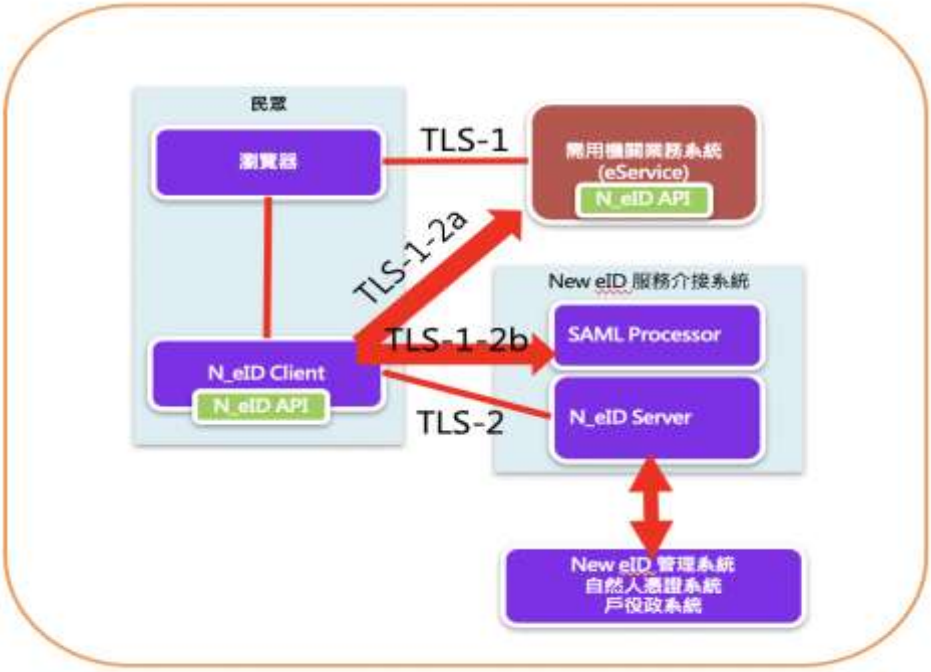


圖 10：通訊安全

1. 加密保護 Encryption

在建立 eService 與 N_eID Service 之間的信任關係期間，雙方必須交換必要的密鑰，以便以安全的方式加密 SAML 訊息。每一方必須創建一個單獨的加密密鑰對，它必須與簽章密鑰對不同。使用 XML 加密建議的算法和密鑰長度。

包含請求的資料的衍生在 SAML 請求中加密。參數 AuthnRequestExtension 必須按照[XML-Enc]中的指定進行加密，並放在參數 EncryptedAuthnRequestExtension 中的 EncryptedData 參數內。

斷言(Assertion)也應按照[XML-Enc]中的規定進行加密，並且必須放在回應參數 EncryptedAssertion 中的 EncryptedData 參數內。

由於 SAML 訊息是高度結構化的，因此靜態對稱金鑰不得用於加密。在協商信任關係期間使用的原始加密金鑰絕不能在任何訊息中傳輸。如果加密技術（例如混合加密）需要，則應傳輸適當編碼或隨機動態密鑰。應該使用混合加密方法。

2. Signature

在建立 eService 和 N_eID Service 之間的信任關係期間，雙方必須交換必要的金鑰以便以安全的方式簽署 SAML 訊息。每一方必須創建一個單獨的簽章金鑰對，它必須與加密金鑰對不同。

在建立信任關係期間使用的原始簽章金鑰絕

不能在任何訊息中傳輸。在處理 SAML 訊息之前，各個接收方必須檢查簽章。

3. URL-Encoding

簽章應該應用於使用此預設文件交換的每個 SAML 訊息。由於此預設文件使用 SAML 綁定中指定的 HTTP 重新轉址綁定，因此 HTTP 重新轉址綁定應將簽章應用於重新轉址的位置字段中的參數 URL-Encoded。AuthenRequest 和 Response 以及標識簽章算法（SigAlg）的 URI 必須按照 SAML 綁定。

4. Channel Binding

N_eID-Client 和 eService 之間的通道 TLS-1-2a 的通道綁定和 N_eID-Client 與 SAML 處理器之間的通道 TLS-1-2b 應使用此預設中定義的 SAML 協議進行保護。eService 只接受並處理綁定到現有 Web session 的 N_eID-Service 的有效斷言。N_eID-Service 僅接受並處理來自授權電子服務的有效請求。

六、New eID Client

N_eID-Client（包含個人端及需用機關端） 若讀取晶片之公開區由使用者直接輸入讀取碼（CAN）讀取，若讀取戶籍區則直接取得。

而讀取加密區則需使用 EAC 在 eService 及晶片卡間進行線上認證，用以對接 N_eID-Server，認證包含 N_eID_API 之所列之必要功能及對應 N_eID-Server 必須具有資料存取層（SAL）及晶片存取相關功能，相關模組

說明如下：

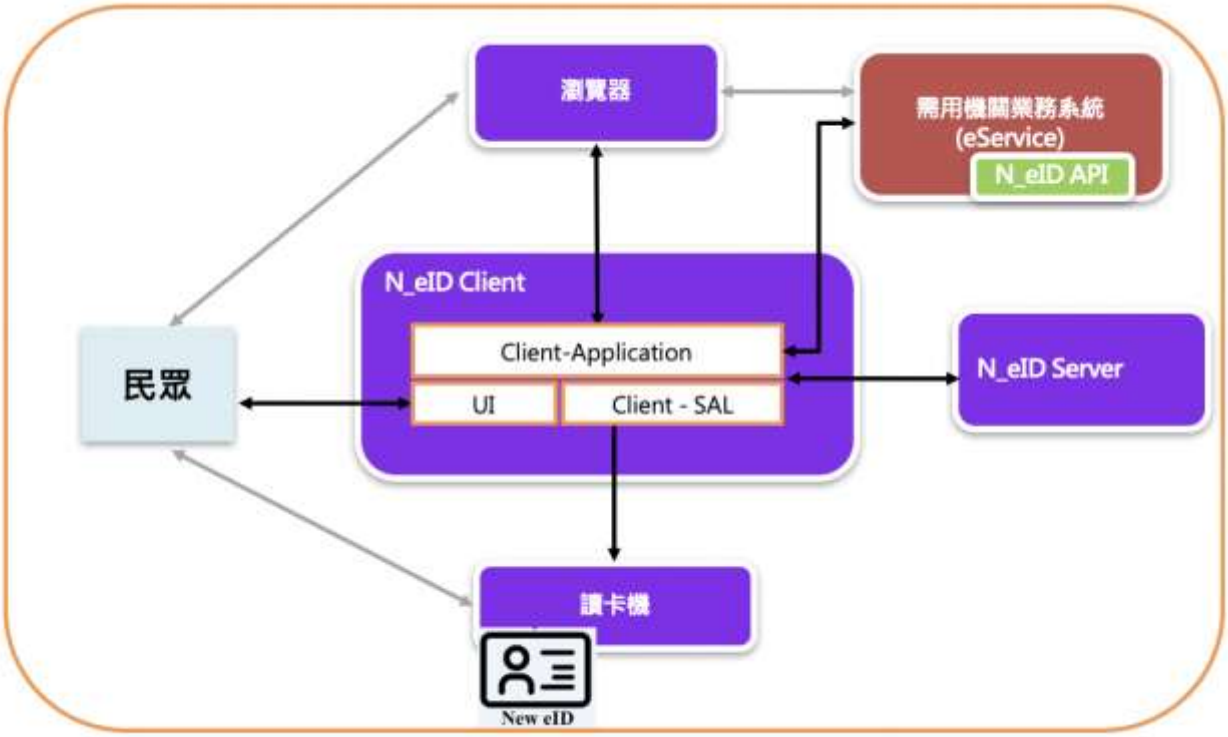


圖 11：N_eID-Client 相關模組說明

(一) N_eID-Client：表示完整之應用端軟體以執行線上認證，可以是單一軟體或分成各個模組軟體。

(二) Client-Application：N_eID-Client 之部分模組，用於與瀏覽器通訊。

(三) Client-SAL： N_eID-Client 之部分模組，參照 N_eID_API 及 IFD-interface 所實作之讀卡機存取卡片及 API 相關功能。

N_eID-Client 可以實作成包含下列不同之模組：

1. Full N_eID-Client：一個獨立運行之軟體，可以於瀏覽器叫用進行線上認證，包含 Client-Application、

Client-SAL 及 UI。

2. eID-Kernel：包含 Client-Application 及 Client-SAL 用以使用者進行開發整合成使用者之應用程式（Integrated N_eID-Client）。

肆、New eID APP

一、行動身分證功能情境

（一）註冊綁定

圖 12：註冊綁定

1. 由需用者進入 New eID 管理服務之申請網頁填寫申請表。

2. 輸入卡片密碼（PIN1）。

3. N_eID-Client 驗證卡片密碼（PIN1）後申請網頁轉發至 New eID 管理服務。

4. 取得晶片資料拋轉至申請網頁之驗證資訊欄位，完成單因子認證之身分確認。

5. New eID 管理服務系統產製對應 Token 並發送一次性 OTP 簡訊至原申請之手機號。

6. 輸入 OTP 驗證碼驗證無誤後，輸入 Token 讀取碼以取回 Token 值

7. 設置行動 APP 之進入密碼（可以指紋或 FaceID 視需用者手機硬體裝置而定）否則無法使用。

8. 設置行動 APP 產生條碼之密碼（可以指紋或 FaceID 視需用者手機硬體裝置而定）否則無法使用。

（二）個資查詢

圖 13：個資查詢

需用機關如讀取行動身分證 APP，以公開區資料為對象，Open API 無需申請，如以加密區資料為對象，應依據 Secure API 申請作業規範辦理，即需事先填寫申請表說明用途、需用作業系統、IP 位址及相關佐證資料，審核完成配發憑證

1. 民眾輸入進入行動身分證 APP 之密碼。
2. 民眾依需用機關（構）業務需求選擇個資。
3. 民眾輸入產製動態條碼之密碼。
4. 需用機關掃碼後驗證需用機關憑證檢核是否有讀取資料之權限。

5. New eID 身分證管理服務轉發戶役政系統請求個資。

6. 需用機關（構）取得個資。

7. New eID 身分證管理服務推播個資取用通知。

（三）行動臨時身分證

行動臨時身分證須由民眾臨櫃辦理，原已取得行動身分證之民眾於提出 New eID 遺失申請後，原行動 APP 之功能將立即失效，而無行動 APP 之民眾則由戶所人員協助下載進行臨時身分證綁定，相關情境說明如下：

圖 14：行動臨時身分證相關情境說明

1. 由戶所人員操作 New eID 管理服務產製對應 Token 並發送一次性 OTP 簡訊至申請之手機號。

2. 民眾輸入 OTP 驗證碼驗證無誤後，輸入 Token 讀取碼以取回 Token 值。

3. 設置行動 APP 之進入密碼（可以指紋或 FaceID 視需用者手機硬體裝置而定）否則無法使用。

4. 設置行動 APP 產生條碼之密碼（可以指紋或 FaceID 視需用者手機硬體裝置而定）否則無法使用。

二、行動身分證與 N_eID Server 整合架構

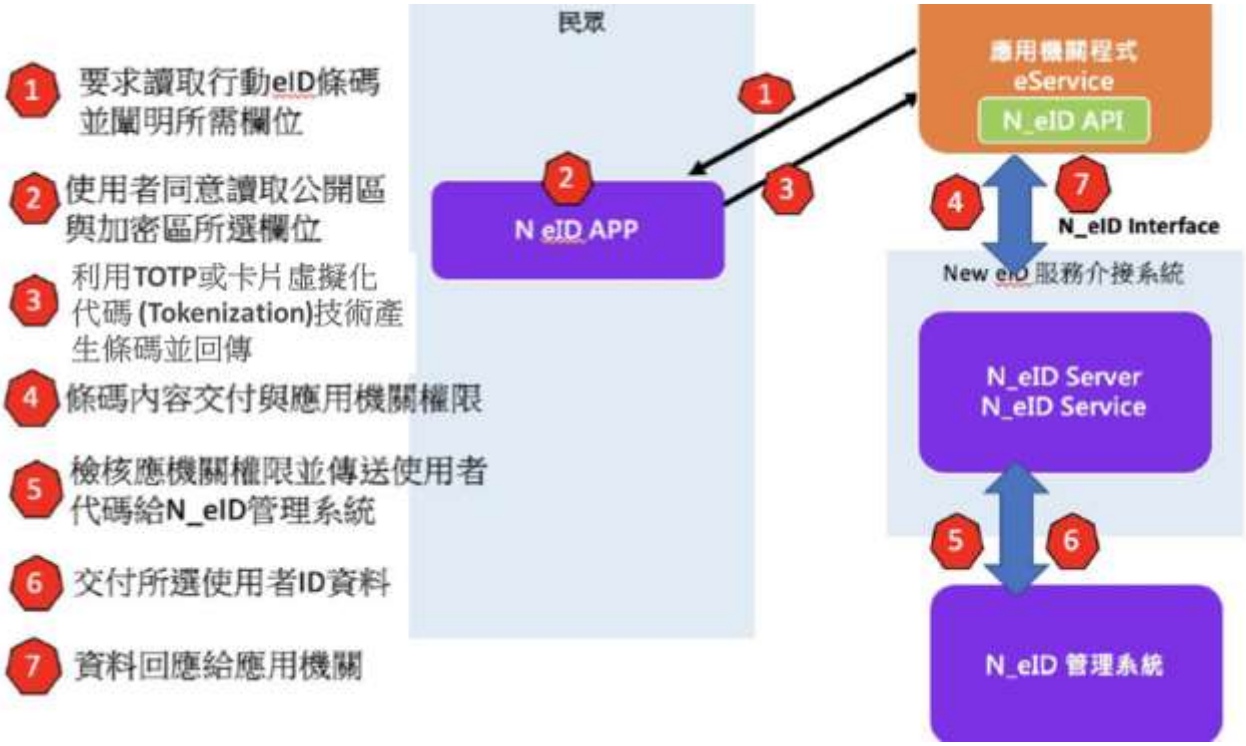


圖 15：行動身分證與 N_eID Server 整合架構

（一）行動身分證若開放第三方開發可以藉由此協定利用 TOTP 或卡片虛擬化代碼 （Tokenization）技術，於 IOS、Android 手機平台上產生一次性密碼。

（二）TOTP 是 Time-based One-Time Password 的簡寫，表示基於時間戳記演算法的一次性密碼進行產製 Standard 1D and GS1 DataBar Symbologies 規格一維條碼。

（三）卡片虛擬化代碼（Tokenization）技術係參照 EMV 國際信用卡組織所定義之代碼化技術規範，可將實體卡片轉換為數位化虛擬卡，於每次認證時產生一次性之安全條碼。使用 Tokenization 技術並產生二維條碼。

三、行動身分證應用程式與系統安全技術要求

本節針對不同面向之行動應用程式安全訂定技術要求，其中包括五大面向：「行動應用程式發布安全」、「安全敏感性資料保護」、「交易資源控管安全」、「行動應用程式使用者身分鑑別及授權與連線管理安全」及「行動應用程式碼安全」。

(一)行動應用程式發布安全

(二)行動應用程式發布

行動應用程式應於可信任來源之行動應用程式商店發布。行動應用程式應於發布時說明欲存取之安全敏感性資料、行動裝置資源及宣告之權限用途。

(三)行動應用程式更新

行動應用程式應於可信任來源之行動應用程式商店發布更新。行動應用程式應提供更新機制，並於有安全性更新時主動公告。

(四)行動應用程式安全性問題回報

行動應用程式開發者應提供回報安全性問題之管道。行動應用程式開發者應於適當期間內回覆問題並改善。

(五)安全敏感性資料保護

(六)安全敏感性資料蒐集

行動應用程式應於蒐集安全敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。

(七)安全敏感性資料利用

行動應用程式應於使用安全敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。行動應用程式如採用通行碼認證，應主動提醒使用者設定較複雜之通行碼。行動應用程式應提醒使用者定期更改通行碼。

(八)安全敏感性資料儲存

行動應用程式應於儲存安全敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。行動應用程式儲存之安全敏感性資料，應僅用於其使用聲明之用途。行動應用程式儲存之安全敏感性資料，應避免將安全敏感性資料儲存於冗餘檔案或日誌檔案中。安全敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存。安全敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取。安全敏感性資料應避免出現於行動應用程式之程式碼。行動應用程式於畫面擷取時應主動警示使用者。

(九)安全敏感性資料傳輸

行動應用程式透過網路傳輸安全敏感性資料，應

使用適當且有效之金鑰長度與加密演算法進行安全加密。

(十)安全敏感性資料分享

行動裝置內之不同行動應用程式間，應於分享安全敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。行動應用程式分享安全敏感性資料時，應避免未授權之行動應用程式存取。

(十一)安全敏感性資料刪除

行動應用程式如涉及儲存使用者安全敏感性資料，應提供使用者刪除之功能。

(十二)交易資源控管安全

1. 交易資源使用

行動應用程式應於使用交易資源前主動通知使用者，並提供使用者拒絕之權利。

2. 交易資源控管

行動應用程式應於使用交易資源前進行使用者身分鑑別。行動應用程式應於使用交易資源後紀錄使用之交易資源與時間。

(十三)行動應用程式使用者身分鑑別及授權與連線管理安全

1. 使用者身分鑑別與授權

行動應用程式應有適當之身分鑑別機制，確認使用者身分，並依使用者身分授權。

2. 連線管理機制

(4) 行動應用程式應避免使用具有規則性之交談識別碼。

(5) 行動應用程式應確認伺服器憑證之有效性。

(6) 行動應用程式連線使用之伺服器憑證應為可信任之憑證機構所簽發。

(7) 行動應用程式應避免與未具有效憑證之伺服器，進行連線與傳輸資料。

(十四)行動應用程式碼安全

1. 防範惡意程式碼與避免資訊安全漏洞

行動應用程式應避免含有惡意程式碼。行動應用程式應避免資訊安全漏洞。

2. 行動應用程式完整性

行動應用程式應使用適當且有效之完整性驗證機制，以確保其完整性。

3. 函式庫引用安全

行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本，更新方式請參酌 1.行動應用程式發布安全。

4. 使用者輸入驗證

行動應用程式應針對使用者於輸入階段之字串，進行安全檢查並提供相關注入攻擊防護機制。

(十五)伺服器端資訊安全技術要求事項

本規範旨在針對行動應用程式安全提出基本資訊安全要求，如行動應用程式涉及伺服器端之資訊安全需求，建議應由業者自我宣告或切結其伺服器端資訊安全防護與管理措施，或對於其伺服器端服務之資訊安全防護與管理，出具第三方檢測通過證明。

1. 伺服器端安全管理

伺服器端安全建議應以提供之應用與服務為出發點，進行應用與服務整體之威脅模型分析，找出對服務造成的安全性風險，以實施必要與有效的後續管控措施。

2. 伺服器端安全檢測

行動應用平台伺服器端本質為網站及 Web Service 伺服器，若無適當的安全設計與開發，同樣會存在傳統網頁應用程式所具有的弱點。因此，在伺服器端的安全檢測，建議開發商可斟酌採用滲透測試方式進行檢測。

3. Webview 安全檢測

行動應用程式應使用 Webview 與遠端伺服器進行網頁資源交換。行動應用程式於 Webview 呈現功能時，所連線之網域應為安全網域。

伍、New eID-Server 安全規劃

一、功能架構

本節介紹 eID 架構中 New eID-Server 的安全架構。模組和通訊通道以邏輯概述顯示。本概述中包含的實體包括：N_eID-Server，eService，EAC-PKI 和民眾 N_eID-Client。

（一）eID 架構概述

N_eID-Server 在 eID 架構中的作用包括：

1.與民眾的N_eID_API實現N_eID-Client進行通訊。

2. 與EAC-PKI的連接，用於驗證收到的資料來自有效的eID，並允許eID驗證eService的真實性。

3. 將線上身分驗證的結果傳輸到eService。

在大多數情況下，eID 架構的所有模組都通過 Internet 進行通訊，使用加密協議進行安全通訊。如下圖所示：

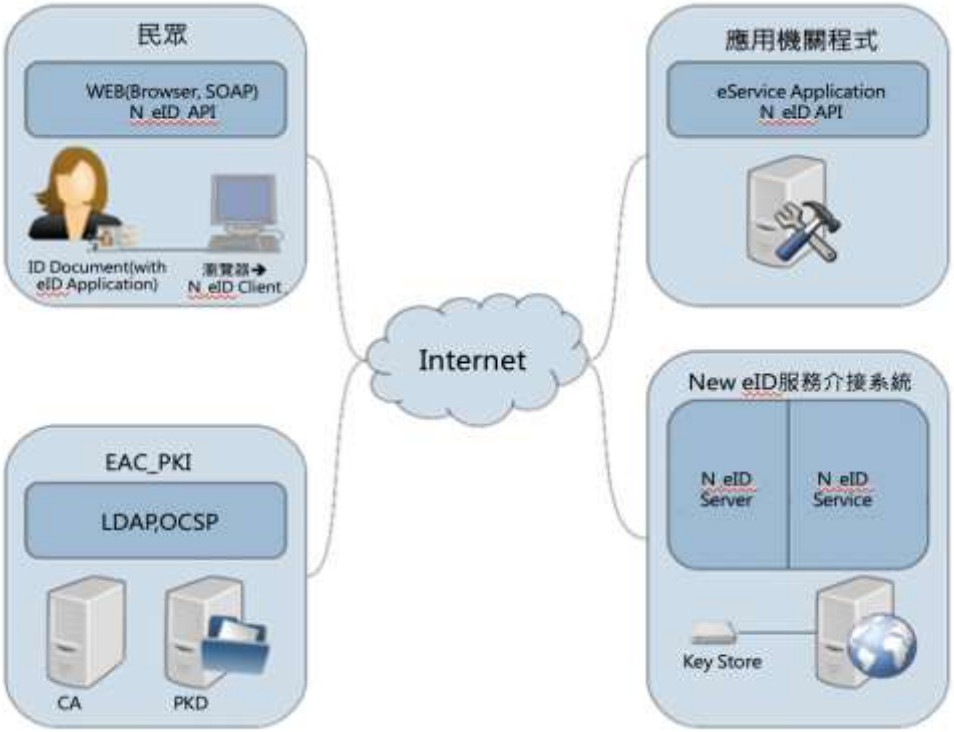


圖 16：Overview of the functional architecture of the eID 架構

eID 架構的功能架構概述，N_eID Server 也可以直接與 eService 通訊。然而，N_eID Server 連接到 Internet 以與民眾的 N_eID-Client 和 EAC-PKI 進行通訊。

N_eID Server 可以由服務提供者在內部操作，的情況下由 e–Service 操作。以下部分簡要介紹典型 N_eID Server 的模組。它們至少包括一台名為 N_eID Server 的伺服器，EAC 應用程式，N_eID_API 和 Web 伺服器正在其上運行。此外，金鑰儲存需要金鑰儲存區（加密器）。

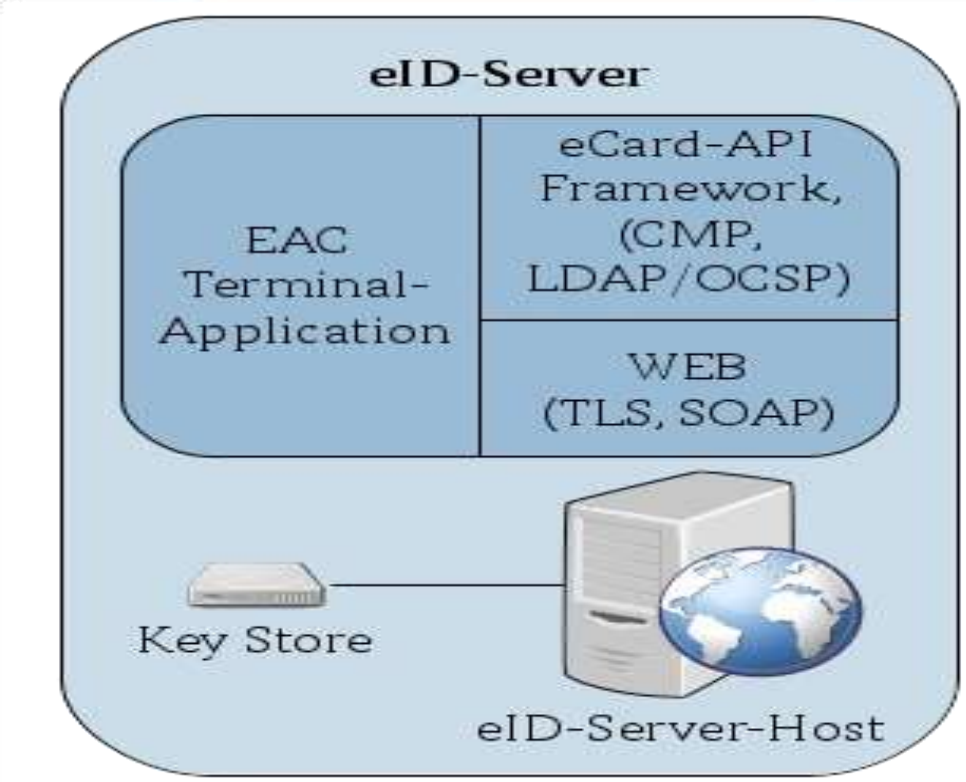


圖 17：Architecture of a typical N_eID Server

（二）N_eID Server 的模組

本節提供滿足 N_eID Server 操作功能要求所需的各種模組的訊息描述。

1. IT 系統

運行 N_eID Server 至少需要兩個 IT 系統：N_eID Server 和金鑰儲存區（加密器）。

(1) eID伺服器主機：N_eID Server是運行N_eID Server（包括EAC終端應用程式，N_eID_API和Web介面）的IT系統。

(2) 金鑰庫（加密器）：金鑰庫是用於簽章創建和存儲終端授權憑證的金鑰的核心模組。金鑰庫直接連接到N_eID Server-Host。

2. 應用

以下部分顯示在 N_eID Server 上運行所需的最小應用程式集。

(1) EAC應用：EAC應用程式使用N_eID_API從eID讀取身分資料，並將這些資料提供給eService的業務邏輯。

(2) WEB：Web服務（WEB）為eService提供接口，封裝eID-Function中的協議和模組。

(3) N_eID_API框架：N_eID Server和N_eID-Client之間的通訊由N_eID_API的實現來管理。

3. 通訊

(1) N_eID Server使用前章的協議透過網路與eID的其他模組進行通訊。

(2) 網路：要將N_eID Server的Web服務提供給eService或連接到User的N_eID-Client，需要Internet存取。出於管理目的，可能需要與本地網路的附加連接。

(3) 協議：N_eID Server，eService和User的N_eID-Client之間的一般資訊流基於使用傳輸層安全性（TLS）的SAML或SOAP或RESTful。

N_eID Server 必須能夠存取 EAC-PKI 的公鑰目錄（PKD），憑證機構（CA）和憑證廢止清冊（CRL）。作為 PKD 存取的替代或補充，憑證可以透過安全機制雙向交換。用於上述目的的協議是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）。為了檢索特定於 eService 的 eID 或憑證狀態，必須支援 GetBlackList，以便檢索受信任憑證的簽章列表（主列表）。

這些要求僅涉及用於衍生存取控制（EAC）的公鑰基礎結構（PKI）。且必須支援 MOICA 的轉換需求並符合 GPKI 的認證協議和組織要求。

二、安全準則

eID-Data，即存儲在 New eID 的民眾的個人資料以及對民眾的 eID 執行的操作的結果，是主要受保護的資產。在 eID 架構的上下文中需要保護的其他資料被分配以保護這些 eID 資料（例如私鑰）。為了保護資料與資訊安全的基本要求，機密性（不洩露資料）和完整性（驗證資料不被操縱以及交易和訊息交換可以信任，即真實性）被認為是最高級別。因此，N_eID Server 的最終安全目標（SO）是：

SO1：必須保證 eID 資料的機密性。

SO2：必須保證 eID-Data 的完整性（包括真實性）。

有關安全目標的更詳細說明，請參閱下表：

表 23：eID 資料的基本安全目標

Security objective	***Description***
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N_eID-Server中超過特定驗證程式所需的時間。
Integrity	必須確保從eID以及與其關聯應用程式和系統（在本例中為N_eID Server）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、安全要求

(一) 組織資訊安全

1. 內部組織 - 角色概念

必須制定並紀錄角色概念，並採用以下原則：

(1) 職責分離

(2) 需要知道的原則

2. 角色排除必須始終遵循以下原則（職責分離）：

(1) 負責人不得執行操作或管理任務

(2) 具有控制任務的人員不得執行操作或管理任務

(3) 管理權限應限於有限數量的人員。下表描述了最小角色集

表 24：角色描述

Role	*Description*
N_eID Server的負責人	負責人對eID服務的組織單位負有一般責任。PiC是IS管理團隊的一部分。
N_eID Server的IT安全官（ITSO）	IT安全官（ITSO）是IS管理團隊的一員，有助於與管理員一起完善系統安全原則。 ITSO與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。
管理員（S）	管理員（最好是：一組）擁有eID服務的所有IT系統的最高權利。管理員負責實施備份，惡意軟體防護和定期更新保護措施（例如惡意軟體簽章文件）。 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。
民眾	eID服務的民眾。這包括使用eService的民眾和eService本身，因為它們都使用N_eID Server進行相互身分驗證。 作為民眾角色不得獲得管理權限。

(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意識培訓，其中涉及考慮安全概念的任務的安全相關性。

必須由負責人定期檢查員工的技術資格，以確定是否需要再培訓。 如果履行內部組織-角色概念（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

存取意味著在 IT 系統上擁有民眾帳戶資料，以便使用 IT 系統的功能。應建立紀錄和審查確保只有經過授權的人員才能進入的紀錄概念。

1. 建立紀錄和審查存取概念。

2. 在存取概念中，必須根據角色概念定義具有保護要求的資料的存取權限。

3. 必須根據角色概念及其排除的要求分配存取權限。

4. 必須確保存取和使用儲存在HSM中的資料（例如私鑰）的管理原則。

5. 使用HSM可能意味著將管理原則衍生到整個eID伺服器。

最低要求是：

(1) 必須定義每個IT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IT系統如何對單個角色進行身分驗證。最低要求是通過民眾姓名和密碼進行身分驗證。因此，必須開發適當的密碼指令。只允許使用強密碼。作為最低要求，必須滿安全密碼使用規則。優先作法應該需要硬體Token和密碼的組合來進行認證。

(3) 遠端管理需要在存取概念中進行適當考慮。必須使用強認證機制和強加密來保護管理的通訊信道。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N_eID Server的所有IT模組。

(5) 民眾不得進入N_eID Server的其他IT模組而不是Web服務。

(6) 必須根據角色概念及其排除的要求分配eID伺服器的許可授權。

(四) 加密

1. 使用加密控制的政策（加密概念）

為了滿足技術指南 N_eID Server 功能規範的加密要求，必須開發關於 eID 服務的金鑰管理和憑證管理的加密概念。此加密概念必須考慮根據自然人憑證規範之金鑰長度和算法以及憑證策略 CVCA 產生的要求。

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) 物理和環境安全

1. 設施存取概念

必須開發和紀錄 N_eID Server 位置（建築物，房間）的設施存取概念。 進入設施的人數應限制在規定的最低限度。

備註：設施存取概念可以是一般存取控制策略的一部分，該策略定義對訊息和訊息處理設施的存取限制。

2. 安全區域 - 物理安全邊界

(1) N_eID Server 操作所需的 IT 模組和技術設備必須託管在建築物內。這些建築物必須提供託管 IT 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告警系統。必須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。這必須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。必須確保在警告管理人員到達之前保護未經授權的入口嘗試。

3. 安全區域 - 物理進入控制

必須檢查，監控和紀錄安全區域的入口和存在。必須建立入口控制技術。

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 IT 系統的安全區域。

(2) 所有其他角色和外部人員（例如訪客）必須由管理員持續護送。

(六) 運營安全

1. 操作程序和責任-變更管理

必須建立變更管理。這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 N_eID Server 的所有 IT 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無可挽回地刪除（例如，破壞硬碟）。

2. 防範惡意軟體

除 HSM 之外的所有 N_eID Server 的 IT 系統都必須配備活動的惡意軟體掃描程式。僅允許使用經檢查的無惡意軟體資料媒體。使用過的惡意軟體簽章文件必須是最新的。

3. 更新軟體

必須在 N_eID-Server 的每個 IT 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. 紀錄和監測

N_eID-Service 的每個 IT 系統都必須具有日誌紀錄功能。至少必須紀錄以下事件：

(1) 系統登錄（成功和失敗）

(2) 存取嘗試

(3) 每個管理存取權限

(4) 通過Web服務進行的每次存取

如果超過 3 次不成功的系統登錄嘗試，則必須產生警報。管理員必須捕獲此警報。在這種情況下，管

理員必須讓資訊安全人員決定進一步的程序（例如關閉 eID 伺服器或重置帳戶）。

5. IT 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 IT 系統。這意味著必須考慮有關安裝和操作的民眾指南的所有說明。

必須基於最小化/強化的操作系統來安裝和操作每個 IT 系統。這意味著只使用 eID 服務所需的服務。不得安裝 N_eID-Server 不需要的軟體。

必須以所有角色僅獲得所需最小權限的方式完成權限分配。必須紀錄權限分配。

適當的措施（例如 BIOS 設置）必須強制只能從指定的媒體（例如特定的硬碟驅動器）進行系統啟動。

必須以符合存取概念和存取概念的識別和授權機制的方式預設操作系統或應用程式。

6. IT 系統的完整性保護

必須至少每週檢查一次 eID 服務的每個 IT 系統的完整性，採取適當的措施。必須紀錄檢查結果。

如果完整性檢查失敗，則必須關閉受影響的 N_eID-Service IT 系統。如果適用，必須根據可用性概念啟動冗餘模組。

(七) 通訊安全

1. 網路安全管理 - 網路安全區域

N_eID Server 的本地網路必須分為三個安全區域：

(1) Internet區。

(2) 外部區域（即DMZ）。

(3) 內部區域。

必須透過防火牆系統實現這些區域的分離。

N_eID Server 必須分成兩個獨立的物理模組，即 eID Web 伺服器主機（即 Web 前端）和 eID 應用伺服器主機（即應用伺服器）。eID Web 伺服器主機必須放在外部區域中，並且 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。

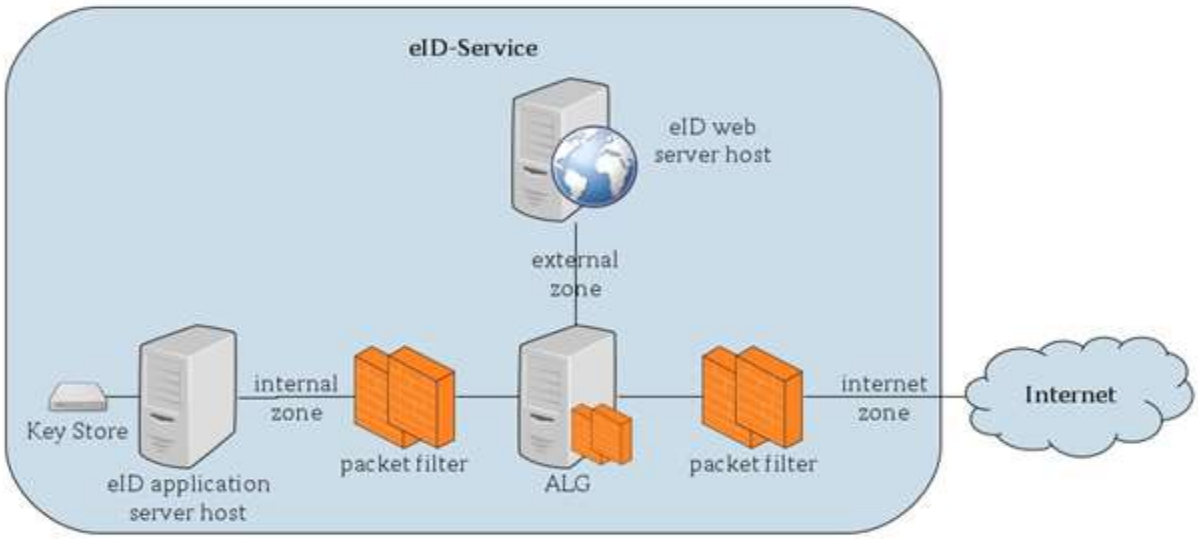


圖 18：本地網路的分離

2. 網路安全管理 - 防火牆系統（安全閘道）

如上圖所示：本地網路的分離顯示，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。它必須設計為封包過濾器（PAP），網

頁應用級閘道（ALG）和另一個封包過濾器（PAP）的組合。

必須預設防火牆系統，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，防火牆系統必須紀錄所有連接。

必須定期檢查日誌文件，至少每天檢查一次。必須評估檢測到的攻擊和攻擊企圖，並且必須進行適當的反應。如果紀錄功能失敗，則必須向管理員發送警報。如果管理員無法重新啟動日誌紀錄功能，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）。組織和技術措施必須確保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-外包

如果 eID 伺服器由代表 eService 的第三方（eID 服務）託管，則與外包 eService 的協議安排必須包括 eID 服務的承諾，以滿足本技術準則的安全要求。

(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。

陸、外部 API

本節 API 架構規範訂定 eService, N_eID-Server 與 N_eID_Client 所有對應的 API 參考，包含了 Open ,Secure API 與自然人憑證之 PKCS11 無縫接軌之 API 相關細部項目，未來可依據得標廠商與晶片廠商對此架構做相關的微調與修改。此參考也依據了(ISO 24727 ICC programming interfaces）的規範定義。

柒、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，若不希望請刪除行動電話）

6. 民眾憑證重寫

7. 查詢民眾憑證狀態

8. 修改憑證公佈狀態

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. 修改憑證公佈狀態

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（無個資）。

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（無個資）及掛失（撤掛）註銷名單（無個資）。

(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 PKI 金鑰（2 把 RSA 及 3 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。

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	卡應用服務存取	初始化
		終止

（以 New eID Applet 功能為主）		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	IsKeyUsageEncipherment
	確認憑證金鑰用途函式：IsKeyUsageKeyAgreement	IsKeyUsageKeyAgreement
	取得憑證的 CRLDistributionPoints 函式	GetCRLDistributionPoint
	取得憑證的 SubjectDirectoryAttributes 子項目之一 subjectType（主體型別）函式	GetSubjectTypeOID
	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SubjectDirectoryAttributes子項目之一，憑證類別代號函式	GetCertTypeID
	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	GetKeyUsage
	取得憑證 AuthorityInfoAccess 函式	GetAuthorityInfoAccess
	GetSubjectDirectoryAttribute	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	OCSPCheckSN
	線上憑證狀態查詢函式（OCSP）：OCSPCheckCert	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	

捌、 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，英國與法國的 eID 整體架構規劃。有鑒於歐盟 eID 建立已有多年經驗，故本案 API 文件參考歐盟高安全標準建置方式（LOA：High）提供。

茲我國 New eID 系統，須以最安全與便民之考量建構此數位身分識別證整體架構，綜合前述之方案，提供結論與建議如下：

一、eID 整體架構可參考 SOAP 與 SAML2.0 規範，亦可參考 OAuth2.0 的 Open ID Connect 規範建置，但因為歐洲各國使用 Open ID connet 架構國家不多，且除

XML 方式，未來建置廠商也可以思考依據效能改用 RESRful 架構完成。由於新技術演進速度非常的快，某些應用標準實際上也可按照 SAML 邏輯建置。

二、因內政部亦為使用 New eID 之需用機關，所以 N_eID-Server 採用之認證與管理方式（SOAP 或 SAML）、對外公告之 API 及需用機關的架構模式，建議內政部先行建置，其他需用機關則可依循相關模式，再根據其業務系統特性進行調整建置。

三、由於 New eID 為新建立之架構，其內部導入了對應之 Document 憑證管理機制，此架構已在護照應用有良好之處理架構與流程，歐盟大多數國家也依據此架構作為 eID 衍生架構，故 API 建置建議須按照國際標準開發對應 API，以因應未來多元需求可方便導入。

四、另本案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驗證與管制，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，又個資保護責任在於個資需用機關，內政部只檢核授權狀態，不紀錄個資作業細節，以釐清個資保護責任歸屬

第柒章、自然人憑證規劃

現行自然人憑證建置案採整體委外方式，將卡管中心及 IC 卡供應機制管理等相關事宜皆委由廠商負責統籌執行，並依照內政部 IC 卡及讀卡機價格審議小組議定之價格收費，由戶政事務所（含辦事處）代收 IC 卡之卡片工本費用，並非規費。隨著數位身分識別證（以下簡稱 New

eID）換發，將結合憑證規劃，於晶片內存放自然人憑證，並可由民眾依其意願選擇是否使用憑證功能。

自然人憑證規劃報告就 New eID，應採新建發證系統或整合現行自然人憑證發證系統，或其他更好可行方案，及其衍生之相關議題，進行詳細規劃評估。

壹、 新舊憑證整合機制

關於新舊憑證之區分、並存或取代以及移轉等議題，其前提依 New eID 晶片內所存放憑證，係採新建發證系統抑或整合現行自然人憑證發證系統而有所不同，是以下先針對新建發證系統抑或整合現行自然人憑證發證系統評估並提出建議。

一、憑證發證系統方案規劃

新建發證系統抑或整合現行自然人憑證發證系統評估憑證規劃有二方案。

方案一擴充案：

為沿用現有之自然人憑證管理中心，整合現行自然人憑證發證系統，修改現行內政部憑證管理中心憑證實務作業基準（Ministry of the Interior Certification Authority Certification Practice Statement , MOICA CPS，以下簡稱憑證實務作業基準），並核發憑證至 New eID 內。

方案二新建案：

為新建憑證管理中心核發憑證至 New eID 內，現行自然人憑證發證系統漸次退場。以下將從建置時程與成本、法規調適、技術規劃等面向分析，以提供評估建議。

表 25：憑證發證系統評估

條件	方案一擴充案 整合現行自然人憑證發證系統	方案二新建案 新建發證系統
技術	• 晶片載體更換，應用機關之 AP 須配合修正 • 憑證信賴路徑與現行憑證相同	• 配合 New eID 晶片載體 ，應用機關應開發新 AP • 需重新佈建憑證信賴路徑，且舊憑證信賴路徑需一併整合
成本	成本較低	成本較高
法規	• 調整現有憑證實務作業基準 • 憑證實務作業基準需送審	• 撰寫新憑證實務作業基準 • 憑證實務作業基準重新送審，預估時程較長
操作	• 修改既有 CA 系統	• 建置新 CA 系統而舊 CA 仍需維運至一定期限
時程	• 系統建置時程約 0.25 年 • 上線程序約 0.5 年	• 系統建置時程約 0.5 年 • 需通過 EAL 5+（含）、WebTrust 認證，從稽核準備到取得認證，需一年以上時間 • 上線程序約 1 年以上
優點	毋庸考量退場機制	重新設計更為開放的技術與介面
綜合評論	• 成本、時程上較優 • 信賴路徑毋庸重新佈建，無新舊憑證管理中心銜接問題 • 自然人憑證晶片載體與舊有自然人憑證不同，得以克服舊憑證未能開放之相關爭議	• 可重新設計更為開放的技術與介面 • 新建憑證管理中心須投入更多成本與時程以及重新佈建信賴路徑 • 須處理舊自然人憑證退場機制
結論	由於 New eID 採用之新晶片已能克服舊自然憑證未能開放 API Source code 程式原始碼之爭議，此技術障礙將不具備。考量上線	

	時程及後續處理事項之簡化，建議採取方案一擴充案，整合現行自然人憑證發證系統。

由於 New eID 採用之新晶片已能克服舊自然憑證未能開放 API 之爭議，且考量就現有應用機關衝擊以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，故建議採取方案一，整合現行自然人憑證發證系統。

二、新舊自然人憑證規劃方案評估

因應 New eID 憑證載體變更，則應用機關之應用系統則須介接新卡片需要至少一年以上準備時間，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。

再擴充現行之自然人憑證管理中心之規劃下，建議採取一人多憑證之開放政策，憑證本質係身分識別及簽章工具，參照實務上一人擁有多顆印鑑，可自行依據不同用途，選擇使用哪顆印鑑，是具有印鑑性質之憑證，應可比照印鑑使用方式，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，對於現今公務使用便利性較高。基於本規劃採取現行自然人憑證擴充建議考量，即現行之自然人憑證晶片卡維持發行，以兼顧非我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。

憑證有效期屆滿不需換卡只需等待現有之自然人憑證到期即可，仍可繼續利用原自然人憑證存取相關資訊系統介接，惟因 New eID 晶片載體更換，仍需配合訂定相關 API 及修改相關憑證作業實務作業基準。

卡片營運屬於 New eID 管理單位權責，包括：用戶網站解鎖卡、修改 PIN 碼、停復用等需，卡片及卡管採購單位提供相關功能予用戶。

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

(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、卡管中心規範

(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：

規劃上原則以資訊安全保障為前提，其金鑰安全應該為首要考量因素，故建議採取於卡片內產生金鑰對。

表 26：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	強化相關安全配套機制

	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	

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。

於此，集中製卡中心乃協助憑證作業相關事宜，是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，而 New eID 管理系統即本案所指之卡管中心。

(二) 卡管中心之職責

卡管中心關於憑證項目負責產製用戶之金鑰對、以初始碼設定卡片之初始 PIN 碼、統一初始化符記、提供開通資料管理作業、提供解鎖管理作業以及卡片管理，而金鑰管理系統則由 New eID 管理系統控管。

(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雲資源池來支應，因此就運算資源所需之硬體設備包含異地備援規劃，均配合內政雲資源池所做的規劃，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（含展期）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，屆期可辦理一次憑證展期，第一次憑證展期可延展 5 年，年限總計 10 年，且憑證展期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,如英飛凌 TPM 案件即係啟動軟體更新或更換憑證卡以降低相關資安風險。

憑證展期作業至少提供臨櫃辦理或線上憑證展期等兩種辦理方式，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展期時，為確保資訊的準確性，本案規劃民眾需採戶政事務所辦理方式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。

若民眾是在 New eID 卡發放時選擇暫停憑證使用時，則憑證效期與卡片效期相同，亦即憑證效期不得超過卡片金鑰載具效期，恢復使用期間亦須配合卡片金鑰載具效期。

當發放 New eID 給 65 歲以上民眾時，其 New eID 卡片效期得設為可超過 10 年或永久有效。對於此類 New eID 卡片金鑰載具效期超過 10 年的情況，其憑證在展延為 10 年且到期後將不得再次進行展期作業。若用戶仍有簽發憑證之需求時，則必須換發新 New eID 卡片。而如係發放 New eID 予 14 歲以下民眾，則配合 New eID 規範 14 歲以下民眾須於五年換證之規定，其就領證年紀為 14 歲以下民眾自然人憑證使用效期為 5 年且不得展期。

二、憑證換發作業規劃

民眾如本已取得現行自然人憑證，則於 New eID 換發亦申請憑證，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) 初始個人識別碼規劃

本案規劃採製發 New eID 卡片時即將憑證寫入晶片，並起算憑證效期。其憑證之初始個人識別碼

（以下簡稱 PIN 2 碼），規劃有以下兩方案，說明如下：

1. 密碼函

先以亂數設定 PIN 2 碼，民眾於戶政事務所領取 New eID 卡片，而民眾於戶政事務所領取 New eID 時，戶政事務所人員將發給民眾密碼函，由民眾事後進行變更密碼。

2. 預設密碼

初始密碼為亂碼，申請人於領取 New eID 時，會給予 1 份確認單，確認單上載有預設之用戶代碼。申請人須以該戶代碼設定 PIN2 碼才可使用（即個人自訂密碼 6-12 數字碼）。

然為配合憑證原則開通之規劃，並兼顧民眾資料自主權，本案規劃民眾得選擇暫停使用或廢止憑證。

(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後新 NeweID 的憑證簽發作業。

本案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，建議需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。

本案規劃憑證管理中心在用戶申辦憑證展期作業時，應提供用戶可採線上直接辦理憑證展期作業，或至戶政事務所辦理憑證展期作業的方式。

同理，憑證管理中心在用戶申辦金鑰重新產製及憑證重發作業時，應提供用戶可採線上直接辦理憑證重發作業，或至戶所辦理憑證重發作業的方式。

前述用戶申辦憑證展期作業及金鑰重新產製與憑證重發作業之相關辦理程序及規定，亦應於憑證管理中心憑證實務作業基準中敘明。

(三) 憑證換發對象

現行憑證實務作業基準規定申請人的年齡為 18 歲以上，設有戶籍之國民，且未受監護宣告者，而配合 New eID 全面發放，其憑證申請年紀不再限於 18 歲以上，惟民法上關於未滿 7 歲之未成年人，屬無行為能力，故自身之簽章不具法效力，是以其針對 7 歲以下未成年人是否僅核發簽章憑證，有下表二方案，說明如下：

表 27：7 歲以下未成年人簽章憑證方案

	方案一（7 歲以下不核發簽章）	方案二（全面普發）
優點	1. 保障無行為能力人（7 歲以下） 2. 杜絕未成年使用憑證簽章之法律行為問題所衍生之爭議 3. 限制行為能力人（7-20 歲）之簽章由法定代理人同意申	1.使未成年人及其法定代理人保有使用線上服務需求 2.簽章憑證為中性之工具，簽章之法律效力回歸應用機關按其法律行為（如民法、公投法 18 歲）進行判斷

	請，讓法定代理人具有雙重把關	3.同時簽發憑證可讓管理程序一致 4.用系統依據業務需求決定是否使用 7 歲以下者簽章憑證
缺點	1. 未成年人亦有使用線上服務之需求（例如開立銀行帳戶、連署），此方案將造成使用上不便 2. 身分識別憑證及簽章憑證生命週期不一，需另訂控管機制 3. 事後年滿 7 歲則需重回戶政事務所簽發簽章憑證，造成民眾及機關負擔 4. 應用機關無法依業務需求決定是否使用 7 歲以下者簽章憑證	1.應用系統須特別識別是否為無行為能力 2.使用者須簽屬多張簽章憑證

然而觀察目前實務上，如保險實務上未滿 7 者之被保險人乃由法定代理人代簽被保險人姓名、開立兒童帳戶須要未成年子女印鑑、未成年申請印鑑證明以及戶政事務所辦理遷入登記，皆須要未成年子女之印鑑，是以縱使無行為能力者仍有具備印鑑之需要，因此無行為能力人仍有使用具有印鑑性質之簽章憑證之需求，且隨著且因應純網銀趨勢，其無行為能力係有使用簽章憑證之情境，故應基於簽章憑證為中性之工具，簽章之法律效力回歸應用機關按其法律行為判斷，其相關運用作法建議，透過法定代理人及未成年子女 New eID 加密區個人資料及父

母欄位可交叉比對親屬關係，並透過憑證及數位簽章進行本人及法定代理人數位文件簽署。

肆、憑證實務作業基準修訂

經評估本案建議採取方案一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，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 年可展期 5 年共 10 年，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。

依此，政府機關公開金鑰基礎建設憑證政策建議配合延長為間隔超過 10 年，始須重新辦理身分鑑別程序。

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，其由戶政事務所受理 New eID 之申請，由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 New eID 之負責

之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。

其申請人年紀不限 18 歲以上，其簽發憑證流程將配合 New eID 申請換發流程修正。且應要求用戶或信賴憑證者針對未成人者應規範其使用權益，以保護未成年。

(二) 憑證之金鑰更換及展期

1. 憑證之金鑰更換

配合憑證效期最長規劃為 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 年可展期 5 年共 10 年，10 年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。

2. 憑證展期

配合憑證規劃使用效期為 5 年，屆期延展時間變更為 5 年，應配合修正為原憑證到期後 5 年內。

至於領證時年紀為 14 歲以下者，將不提供憑證展期作業，配合卡片載體更換，重新發放新憑證。

四、金鑰使用期限

配合憑證效期規劃，修正為使用期限 5 年，得展期一次，為期 5 年，共 10 年。

五、金鑰產製

因應未來用戶 New eID 如有更換金鑰演算法之情況，金鑰重新產製部分應新增例外可由憑證註冊窗口辦理。以及配合本規劃建議之金鑰載具的金鑰演算法及功能規劃，金鑰長度規劃應納入 ECC-384 金鑰對之選項。

另，依據本規劃報告，建議密碼模組標準應使用通過 Common Criteria EAL 4+（含）以上規範的硬體密碼模組設備。

六、憑證申請程序

因現憑證已載入 New eID 晶片內，於提出 New eID 申請時，一併進行身分確認，無須先向戶政事務所進行身分確認,而係於民眾領取 New eID 一併進行身分識別。當戶政事務所進行接受憑證時，應先確認民眾未受監護宣告，如發現民眾受監護宣告，戶政事務所即應進行廢止憑證。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。

此外因應集中製卡規劃，憑證同於製卡中心製發時寫入 New eID 之晶片內，且憑證規劃採原則開通，而民眾得選擇是否暫停使用，故規劃當民眾於領取 New eID 得表示是否使用，如拒絕則由戶所人員協助關閉憑證功能。依此，簽發憑證程序應配合修正。

因循上開規劃採取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在申請程序，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即時通訊軟體帳號。

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 集中製卡中心負責，於集中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四碼，惟為了加強憑證與 New eID 之關聯，應於憑證內記載 New eID 之證件號碼作為憑證序號，以供連結，故憑證實務作業基準之憑證內容建議增加記載 New eID 證件號碼之規定。

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（PKS#11）中

介介面，再由 Open 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) 依卡片類別分別調用 New eID 中介軟體或自然人憑證中介軟體。

(三) 調用介面（參數）同 New eID 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，可視情況不需在現時導入，可以在未來直接使用新的 PQC 密碼標準。

但是目前 PQC 標準尚待負責制訂密碼標準的 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，而將來可視情況於需在時更換為 ECC 金鑰演算法，是憑證之金鑰載具採 2 組 RSA-2048 金鑰對與 2 組 ECC-384 金鑰[2]，未來如需將演算法切換至 ECC 將比照 RSA 1024 升級至 RSA 2048，整體應用系統升級準備期約 2 年時間，並定期追蹤管理相關進度

二、2 組 RSA 金鑰對的用途分別為：用於數位簽章兼身分認證，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、兩組金鑰對之憑證，並保留另外 2 組憑證空間供未來可彈性使用。

[2] 此外，應 New eID 晶片內自然人憑證區以外使用需求，晶片內規劃寫入第三對 ECC-384 金鑰對。

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、提供憑證更新、展期、線上操作規劃。

五、因國際趨勢多採取用 eID 多採取 ECC，PKI 多採 RSA，兩者混用情形亦有，且因每年皆會評估金鑰風險評估，與 RSA 與 ECC 安全性及處理效率，為增加金鑰更換彈性建議，預先產製 RSA 與 ECC，以配合未來應用需求。

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 2,000 多個線上憑證服務系統造成過大負擔，建議採取擴充現行自然人憑證管理中心，將係現行較妥適之作法。

二、為使憑證管理中心符合憑證政策，且具備應有之安全性，是規範憑證管理中心之職責、作業流程等，另因現行憑證將寫入 New eID 卡內， New eID 規劃採取集中製卡，並由 New eID 管理系統負責控管 New eID 從申請到製證及發放等事宜，New eID 管理系統即須符合憑證實務作業基準之卡管中心作業規範。

三、憑證效期及換發作業即須配合調整，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與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，且搭配 New eID 換發規劃，以及簽章性質，建議全面核發簽章予民眾。

四、建議採取整併現行自然人憑證管理中心，依此檢視 New eID 規劃與現行自然人憑證實務作業基準相牴觸之處，而提出上開調整方向，作為修訂之參考。

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，讓新身分證成為開啟智慧政府之鑰，達成智慧政府便捷智能服務、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分之數位身分識別證。

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、記者會

由於數位身分識別證之卡面設計已有雛型，為使國民知悉 109 年 10 月將進行全面換發，本團隊規劃於 108 年 8 月底前協助辦理 1 場「數位身分識別證宣布記者會」，主要說明新一代身分證主要功能與未來應用，並針對民眾可能的疑慮主動先跟媒體說明，有助於 109 年的正式換發，雙方分工說明如下，惟此記者會嗣後因故未進行辦理：

表 28：數位身分識別證雙方分工說明表

單位	內政部戶政司	國巨
項目	● 新聞稿確認與發佈 ● 記者會場地申請與布置 ● 記者會邀請與執行	● 協助撰擬新聞稿 ● 協助撰擬假新聞澄清稿 ● 協助撰擬 Q&A 集 ● 有必要時，製作記者會所需之圖卡

三、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，本團隊規劃 6 張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 晶片資料分區保護」、「New eID 換發作業方式與時程」、「New eID 掛失完全攻略」及「New eID 兼具數位簽章，功能更多元」。

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 之換發方式並認識 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

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

圖 19：內政部入口網連結示意圖

本案須負責規劃「建置及換發期間 New eID 專屬網站」，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 20：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加密區資料。

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

本案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：

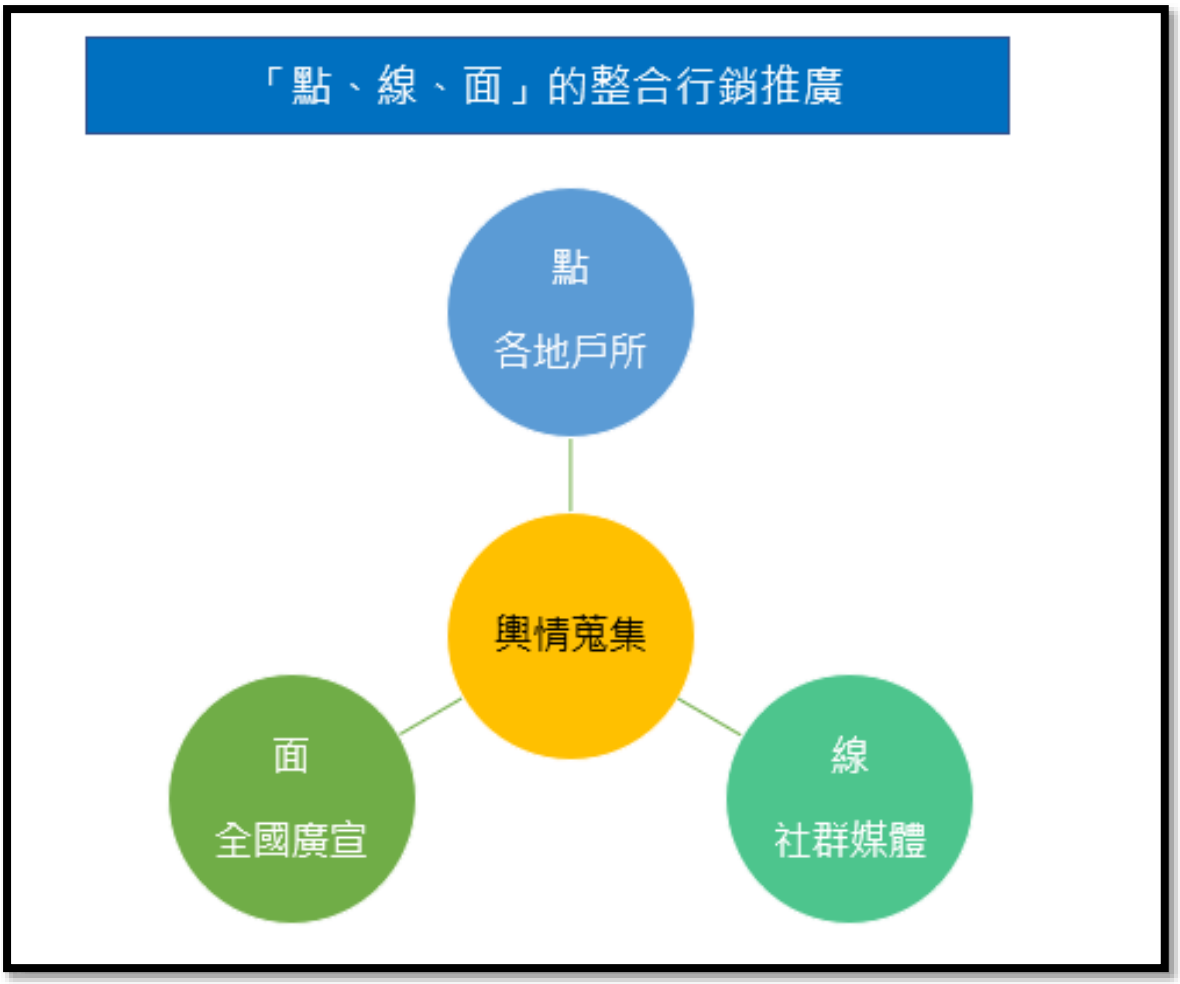


圖 21：「點、線、面」的整合行銷推廣方式

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」這個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 New eID 「LINE@」發布相關訊息。

(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) 由社群小編透過「LINE@」與民眾互動。

(四) 由社群小編負責製作懶人包、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) 於全國重點戲院播放電影開演前的宣導廣告。

(五) 於 6 都的重要大眾運輸工具張貼 New eID 宣導廣告。

(六) 於臺鐵與高鐵車廂內的跑馬燈刊登換發提醒文字。

(七) 於全國性報章雜誌刊登 New eID 宣導廣告或專題報導。

參、109 年廣宣重點

一、109 年廣宣預算分配與廣宣重點建議

(一)「點」→公務行銷：公益託播管道

善用「行政院公益託播」與地方政府的各式公務行銷管道（交通工具、網頁連結、APP 推播、LINE@的提醒、平面與電子廣宣）。

(二) 「線」→以「新全民運動」為主題拍攝換發及體驗影片。

鎖定我國 20~59 歲重度使用網路的族群，拍攝 New eID 換發及體驗影片,在政府機關粉絲專頁或 LINE@好友群組進行宣傳，藉由網路快速傳播的特性，達到社群行銷之目的。影片更可同步應用於內政部與各式公益託播管道共同推廣,建議可由內政部長官或素人拍攝換發及使用體驗影片,並呈現闔家一起申請的議題，形成新全民運動。建議主題如下：

1. 數位身分識別證好處多（開箱文）

主要內容為數位身分識別證換發全流程介紹,並

說明數位身分識別證的各式生活應用。

2. 小朋友如何申請數位身分識別證

可透過家長幫小朋友申請數位身分識別證的過程，宣導 14 歲以下的小朋友數位身分識別證的換發流程與介紹數位身分識別證的好處。

建議可以找網紅拍攝影片以說明使用心得，經評估建議可由「蔡阿嘎」與「那對夫妻」擔任數位身分識別證的網紅代言，說明數位身分識別證的好處，且兩組網紅都是親子一起經營，能夠呈現闔家一起申請的議題，鼓勵父母帶小朋友、年輕網友帶家中長輩一起去換發數位身分識別證，形成新全民運動。

(三) 「面」→全國性媒體：全國性廣播電台廣告。

建議自 9 月起連續透過全國性的廣播電台，例如警廣，持續提醒民眾換發數位身分識別證，相關議題操作建議如下：

1. 9 月份：預告國人加入換證的「新全民運動」

建議由內政部長錄製廣告，預告自 10 月起邀請全民一起加入換證的行列，展現親民與政策執行的決心。

2. 10-11 月份：數位身分識別證好處多

錄製主題以數位身分識別證 4 種申請方式與 8 大好處為主。

3. 12 月份：數位身分識別證謠言終結者。

(四) 設置「New eID 社群經營小組」

因應當前媒體快速傳播與社會訊息的一日數變，建議專案委外執行單位設置「New eID 社群經營小組」，至少需 3 人專責管理，主要負責提供資料給內政部 FB 進行議題操作與錯誤訊息的澄清。

建置 New eID 專屬的「LINE@」進行訊息發布與管理。同時透過輿情蒐集軟體，每天進行輿情蒐集，每週提出分析與預測，並針對異常或緊急事件給予必要之處理（含提供新聞稿、澄清稿及懶人包等），防範未然。

(五) 108-109 年廣宣期程建議

108 年先期作業期間與 109 年 9 月前的換發作業籌備期間，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 10 月開始正式換發作業，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知悉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、規劃內容

(一) 指導單位：內政部。

(二) 主辦單位：內政部戶政司。

(三) 協辦單位：各直轄市、縣（市）政府戶政事務所。

(四) 執行單位：建置案得標廠商。

(五) 單位活動名稱:戶所人員辦理數位身分識別證換發作業教育訓練課程。

(六) 授課對象：各直轄市、縣（市）政府戶政事務所執行本作業之相關人員。

(七) 舉辦方式

1. 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。

2. 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」，透過網站影音或手機APP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 29：戶所人員教育訓練課程表（暫定）

109 年 5-6 月換發作業訓練課程		
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	此部分旨在確保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，協助收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。
109 年 7-8 月上機實作訓練課程		
09：00-10：30	系統功能說明	此部分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 ● 外文姓名登錄 ● 審核結果註記方式
10：40-11：40	數位身分識別	協助戶所人員受理民眾申辦時，能夠迅

	證換發系統作業流程介紹	速且簡易地答覆民眾對於數位身分識別證換發系統基本功能與常見議題之詢問。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，協助收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、各項標準作業程序（SOP）

壹、New eID 印製及品質控管

為確保 New eID 之品質及安全性，針對製卡中心於 New eID 印製過程及品質控管所應遵循事宜，爰訂定「New eID 印製及品質控管標準作業程序（SOP）」，其規劃內容包含製卡過程各階段工作之標準程序，以確保印製品質，且採取安全的方式確保印製階段並無資料外洩，規劃之相關作業範圍如下：

一、空白卡初始化作業。

二、半成卡入庫及結單。

三、半成卡個人化作業。

四、成卡品質檢測。

五、壞卡及報廢卡之銷毀作業。

六、成卡之包裝及入庫作業。

貳、空白卡（含晶片）生產及運送安全控管

為確保 New eID 之品質及安全性，針對製卡中心向卡廠採購所需之空白卡（含晶片）時雙方所應遵循相關生產及運送安全控管等事宜，爰訂定「空白卡（含晶片）生產及運送安全控管標準作業程序（SOP）」，俾利製卡中心向卡廠採購空白卡（含晶片）之過程得以受到控管，以確保空白卡（含晶片）採買以及運送過程的安全性，規劃之相關作業範圍如下：

一、製卡中心辦理空白卡（含晶片）之採購作業。

二、卡廠辦理空白卡（含晶片）生產及運送作業。

三、內政部實地稽核作業。

參、New eID 全面換發作業規劃報告書

為順利於 109 年 10 月起全面換發數位國民身分識別證並結合自然人憑證之數位身分識別證（以下簡稱 New eID），明定相片影像規格、申請與領取作業、通知書、申請書，並規定戶政事務所例行辦理新身分證之掛失及初、補、換領作業，特訂定本作業程序。

一、New eID 全面換發作業程序規劃

(一)換發對象

(二)期程規劃

(三)規費收取

(四)全面換發流程

(五)瑕疵 New eID 處理

(六)統計作業

(七)運送作業

(八)相片規格

二、New eID 掛失及初、補、換領作業及安全管制程序（例發期間）

(一)例發期間之作業內容

(二)New eID 初、補、換領及掛失作業流程

(三)安全管制程序

肆、API 介接申請及應用管理

內政部所推出之數位身分識別證（簡稱 New eID）讀取 API 元件，係可提供各應用服務需求開發者（以下簡稱「開發者」）如個人、機關單位或組織團體進行整合介接，以利各需求端快速開發應用系統，拓展 New eID 應用範圍。為明確開發者就前開 New eID 加密區資料讀取權限之申請及應用管理事宜，特制定「API 介接申請及應用管理標準作業程序（SOP）」，使開發者得依標準程序提出申請並獲得使用授權，進而順利整合及介接 New eID 資料應用程式介面，亦可確保開發者均同意並遵守 New eID 資料應用程式介面使用相關規範，以避免資料遭到非法使用，規劃之相關作業程序包括如下：

一、API 介接申請

(一)申請人（即開發者）區分為以下對象：以資通安全管理法之關鍵基礎設施提供者，並經中央目的事業主管機關指定加密區可讀取欄位；或由個人資料保護法非公務機關之中央目的事業主管機關指定適用行業及加密區可讀取欄位。

(二)申請人應依書面或線上 API 申請書申請使用 API。

二、API 介接申請審查

三、API 介接應用管理

(一)授權使用方式:規範資料交換方式、來源端資訊安全性、安全性傳輸、內政部與授權予開發者之權利與義務。

(二)使用費用：內政部目前無償授權開發者依 New eID API 使用規範所約定方式利用或使用 API，但仍保留未來於公告後收取費用之權利。

(三)開發者應遵守注意事項。

(四)權利歸屬。

(五)責任限制與排除。

(六)授權期間與終止事由。

(七)本作業程序之解釋、適用與修正。

伍、New eID 空白卡及製發安全控管

為確保 New eID 之品質及安全性，針對製卡中心於 New eID 印製過程及品質控管所應遵循事宜，爰訂定「New eID 空白卡及製發安全控管標準作業程序（SOP）」。其規劃內容包含從採購空白卡至製作 New eID 過程之標準程序，以確保原物料採購及製作過程安全性，規劃之相關作業範圍如下：

一、New eID 原物料採購作業（含空白卡及耗材）

二、New eID 製程安檢作業

(一)空白卡（含晶片）安檢作業。

(二)製程安檢作業。

三、產品庫房安全管理

(一)文件紀錄保存。

(二)卡片存放區。

(三)庫房檢核管理。

(四)卡片出入庫管理。

四、耗材安全管制（含入、出庫管理）

五、廢料及廢卡控管（含廢料、壞卡、報廢卡）

六、廢料及廢卡銷毀程序

七、產品委託運送

陸、資安及作業流程管理規則（製卡中心端、卡片端、應用端）

為確保 New eID 整體系統與作業之資訊安全，分別從製卡中心端、卡片端到應用端之資訊安全管理與監控機制，爰訂定「資安及作業流程管理規則」，以此作為相關作業人員遵循之規範，亦可使內政部確保相關作業人員遵守 New eID 資訊安全規範，規劃範圍如下：

一、New eID 管理系統及製卡中心端資安防護規範

(一) 資訊安全通則。

(二) 資訊安全管理。

(三) 安全性檢測。

(四) 資通安全健診。

(五) 資通安全威脅偵測管理機制。

(六) 政府組態基準。

(七) 資通安全防護。

(八) 資通安全教育訓練。

(九) 資通安全專業證照及職能訓練證書。

(十) 災害復原及業務持續機制。

(十一) 資安事件處理機制（含事前、事中、事後）。

二、應用端資安防護規範

(一) 遠端更新資安防護規範。

(二) API 資安防護規範。

(三) 網站安全規範。

三、卡片端安全防護

(一) 晶片安全規範與規格。

(二) 晶片存取安全規範。

(三) 卡片安全性相關規範。