自然人憑證創新應用服務計畫
110-114年度中長程計畫書

壹、 計畫緣起

內政部辦理自然人憑證相關發證及應用推廣業務，於91年研提「自然人憑證發證計畫」、96年研提「自然人憑證發證及應用推廣計畫（97~100年）」、100年研提「自然人憑證創新應用服務推廣計畫(101~105年)」及105年研提「第五階段電子化政府發展工作計畫(106~109年)」，前開計畫於109年度執行期滿，鑑於電子化政府需求，並配合國民身分證全面換發計畫，持續辦理強化自然人憑證應用服務計畫相關工作，惟預期未來自然人憑證客服量將激增及擬採區塊練資訊技術補足個人多元身分識別，加上行動化應用已為未來趨勢，因此將配合行政院「第六階段電子化政府計畫」，以及國發會已研議將「第五階段電子化政府計畫」轉型為「第六階段電子化政府計畫」，本部計畫在110年~114年進行「自然人憑證創新應用服務計畫」，重新規劃執行內容，實現身分多元識別機制，在政府及民間跨域整合服務及打造多元協作環境上，提供必要基礎建設。本計畫除保留現有憑證基本營運外，主要項目包含多元憑證識別行動化跨域應用、推動 AI 智慧型自動化客服及內容傳遞網路 CDN 連結及建置多元身分識別平台，並結合區塊鏈技術強化身分認證服務，最後為因應未來**量子電腦**衝擊研究下一代**後量子密碼學**及115年起憑證是否改用 ECC 演算法簽發以延長憑證效期可行性等方案，期待未來5年應用發展。

貳、 計畫目標（110-114年度）

本計畫分三階段預計五年內逐步分階段達成

一、 第一階段**110-111年**規劃建置 AI 智慧型自動化客服、客戶關係管理（Customer Relationship Management，以下簡稱 CRM）系統、大數據資料庫及分析系統、核發行動自然人憑證及租用內容傳遞網路（Content Delivery Network,CDN）透過網際網路互相連接的電腦網路系統，利用最靠近每位使用者的伺服器，更快、更可

靠地將檔案傳送給使用者，來提供高效能、可擴展性及低成本的網路內容傳遞並提供更好為民服務能量。

二、第二階段112-113年規劃建置多元身分識別平台及導入區塊鏈強化身分識別，將建置相關軟硬體系統，並結合行動自然人憑證增加個人身分識別服務。

三、第三階段114年投入研究下一代憑證演算法及使用核發ECC憑證延長憑證效期可行性與相關憑證應用推廣階段，除上述電子化政府推展機關應用外，擬導入民間創新，以增加應用廣度及深度。

參、實施策略或方法

一、AI智慧型自動化客服建置

（一）前後台軟硬體設備建置。

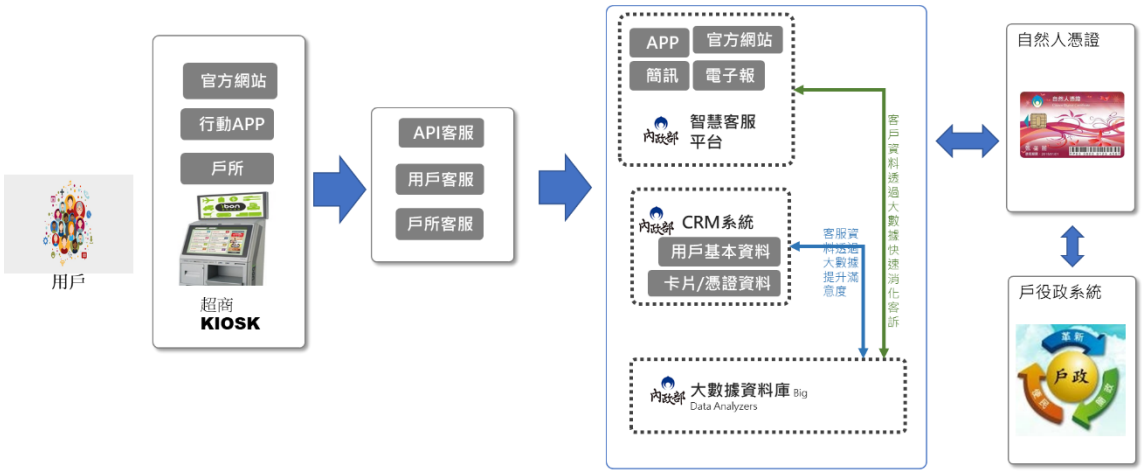
（二）設計開發自然人憑證客服大數據資料庫

（三）整合客戶管理系統資訊至自然人憑證AI智慧客服平台

（四）相關軟硬體設備擬集中化建置於本部資料中心內，方便系統資源統一納管及調度使用。

（五）增設維運及客服人員以維持系統營運需求

（六）整合內政部超商KIOSK平台服務增加服務廣度，如:解鎖卡、修改用戶代碼



二、AI 電子報簡訊平台整合 CRM 系統

（一）前後台軟硬體設備建置。

（二）租用外部大量簡訊服務。

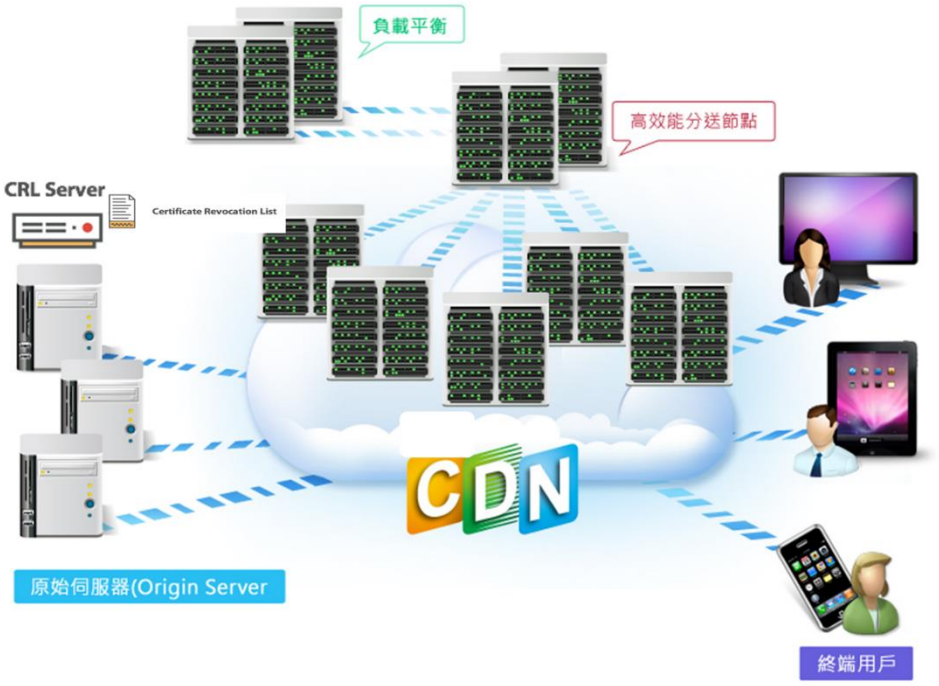
（三）設計開發用戶端憑證資訊通知軟體

（四）相關軟硬體設備擬集中化建置於本部資料中心內，方便系統資源統一納管及調度使用。

三、內容傳遞網路 CDN 空間租用

（一）租用外部 3T CDN 空間服務。

（二）有效分流憑證廢止清冊 CRL、外部宣導影片、內部教育訓練教材及相關憑證檔案。



四、行動化軟體憑證平台

（一）軟硬體設備建置。

（二）相關軟硬體設備擬集中化建置於本部資料中心內，方便系統資源統一納管及調度使用。

（三）建置自動化行動自然人憑證註冊窗口，採以證換證或臨櫃認證後申請自然人憑證。

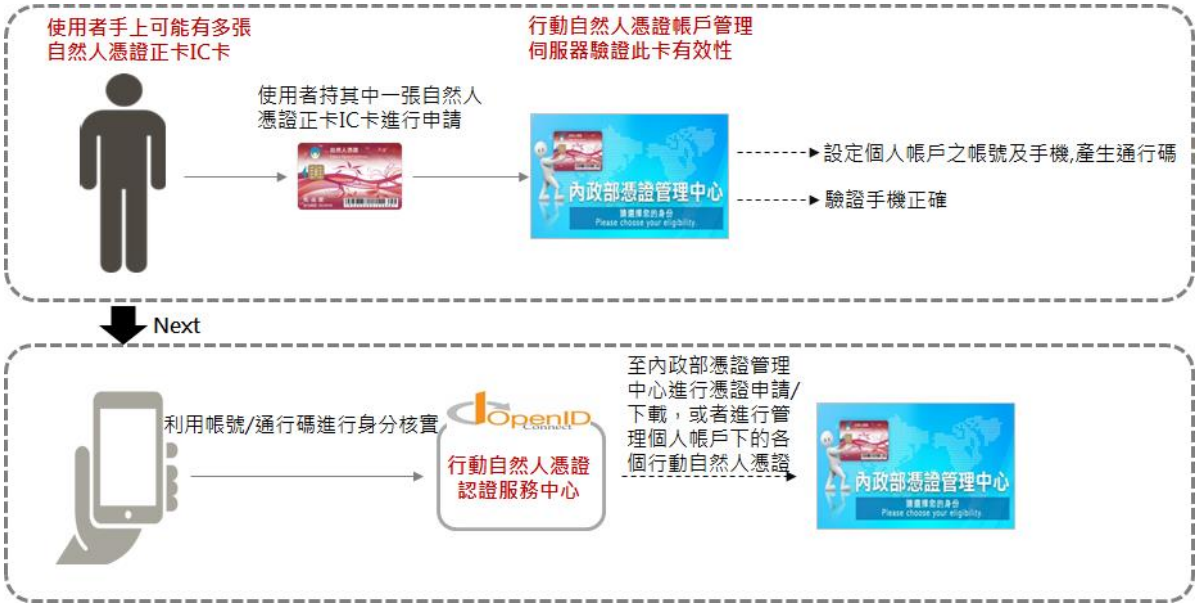
因應行動裝置普及，現行自然人憑證及未來國民身分識別證均為卡片形式難以應用，故提供行動自然人憑證服務於行動裝置上使用。

在此服務中，將建置自動化行動自然人憑證註冊窗口，使用者以線上或臨櫃方式使用本人的一張自然人憑證正卡 IC 卡至行動自然人憑證帳戶管理伺服器驗證此卡有效性，若驗證通過，則設定個人帳戶之帳號及手機號碼，並下載行動自然人憑證 APP。驗證確認使用者身分後，伺服器接著發送驗證手機用之驗證資訊到使用者手機確認為本人使用，若驗證通過，則伺服器發送開通帳戶用之通行碼給使用者。

接著，使用者利用原已設定好的帳號及收到的通行碼到 OpenID Connect 行動自然人憑證認證服務中心進行身分核實，

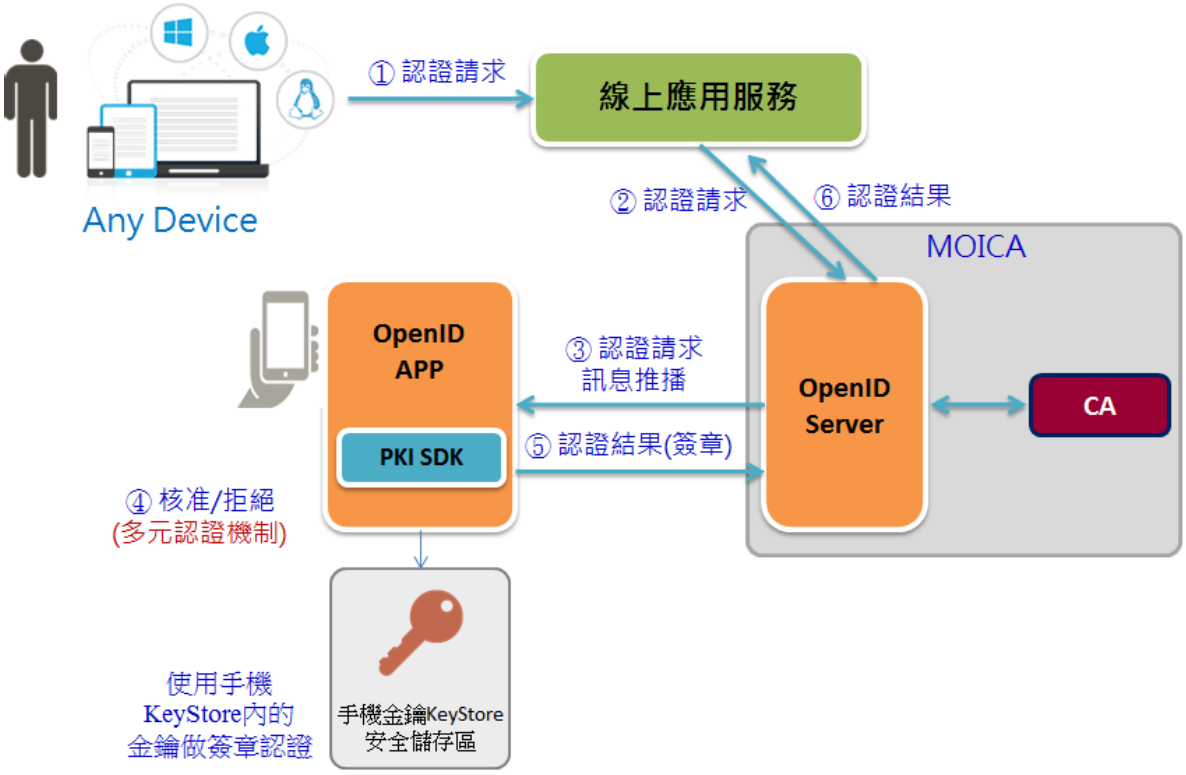
若核實通過，則可至內政部憑證管理中心進行憑證申請/下載，或者在此行動裝置 app 中針對此個人帳戶下的各個不同行動自然人憑證進行內容管理。

其中，針對未來使用者手上可能有多張自然人憑證正卡 IC 卡(例如國民身分證及原本的自然人憑證)，並且可能會申請多張行動自然人憑證(例如使用者有不只一支手機)，故我們提出使用行動自然人憑證帳戶管理功能來處理行動自然人憑證申請/下載，或者管理個人帳戶下的各個行動自然人憑證。



（四）提供符合 OpenID Connect 的行動自然人憑證介接 API。

提供符合 OpenID Connect 的行動自然人憑證介接 API，如下圖，使用者可使用任何行動裝置發送認證請求給線上應用服務，線上應用服務再將此認證請求傳給 OpenID Connect 伺服器，該伺服器將會推播認證請求訊息回使用者手機上的 OpenID Connect App 軟體，該軟體將使用手機金鑰 KeyStore 安全儲存區內的金鑰做簽章認證，並將核准/拒絕認證結果傳回 OpenID Connect 伺服器，並接著傳回線上應用服務。



（五）提供可將金鑰安全儲存於行動裝置機制。

提供可將金鑰安全儲存於行動裝置機制，針對不同手機作業系統，我們均提供將金鑰儲存於手機內的安全區域(SoC)內可達裝置綁定功效。

五、區塊鏈多元身分識別平台建置

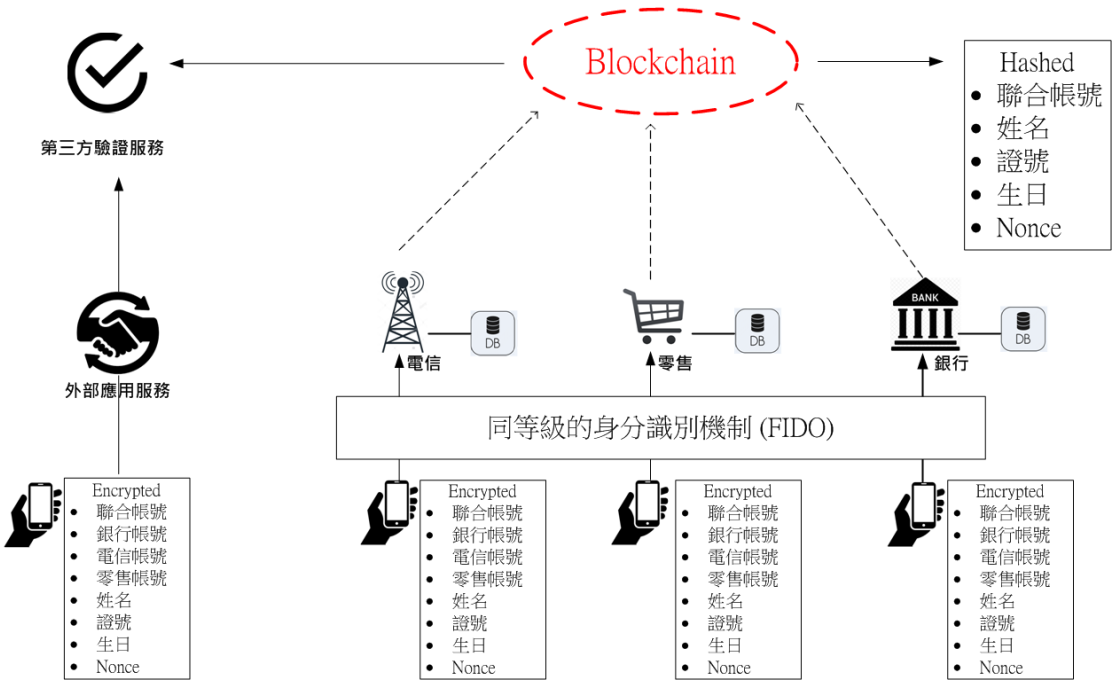
（一）軟硬體設備建置。

（二）相關軟硬體設備擬集中化建置於本部資料中心內，方便系統資源統一納管及調度使用。

（三）介接 T-ROAD 或各單位 LDAP 服務，以擷取用戶屬性資料

憑證主體在網路上之「身分證」，對一個憑證主體而言，其憑證正式主體僅1張，但可能依憑證主體的職業、業務、技能等，可能會有許多情境需確認該憑證主體是否具有某些特性，例如：確認憑證主體是否具備醫事人員、公務人員、勞健保業務承辦人員或者憑證主體是否具備能執行某些業務的資格。

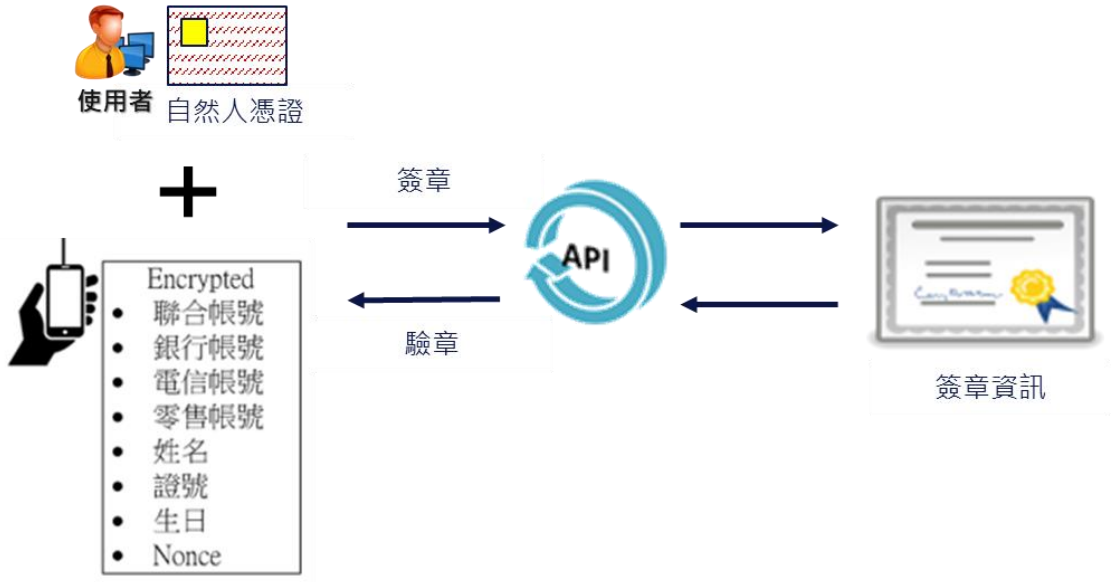
（四）建置區塊鏈身分識別服務系統



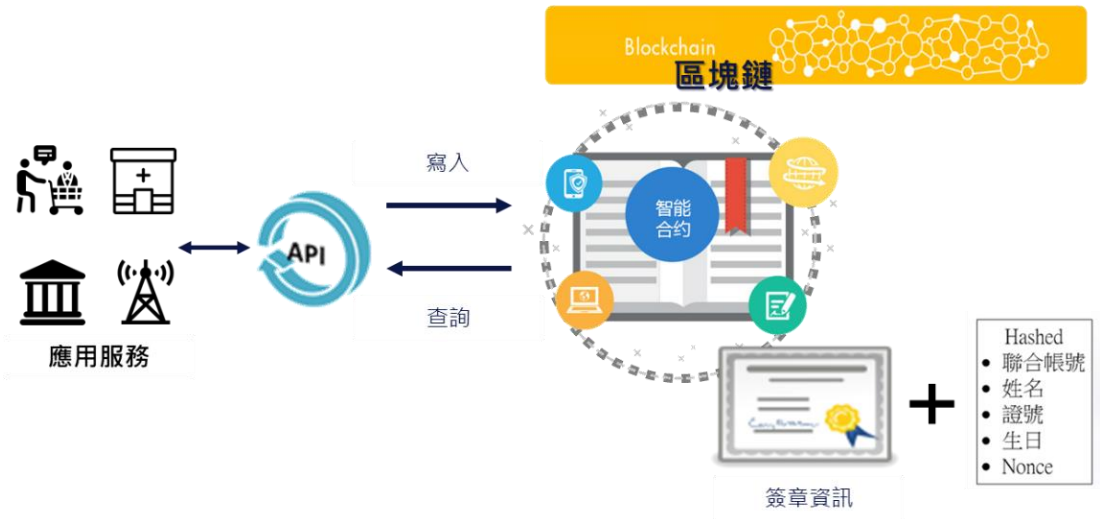
提供以 Ethereum 為底層的區塊鏈系統(Blockchain)，並使用權威證明(Proof of Authority, PoA)共識演算法為基礎，在此運作上限定只有授權過的節點才有產生下一個區塊的權限，藉此機制提供一個更安全、擴展性更高的私有區塊鏈系統，並同時保有公有鏈不可竄改、不可刪除及不可否認的特性。透過區塊鏈技術，本系統將佈建可供區塊鏈交換資料、同步資料及去中心化的節點。亦即所有區塊鏈上的節點，會同步存儲區塊鏈上的所有數據，一份數據將會有 N 個備份(N 為節點個數)。

本系統的目標是希望拓展既有自然人憑證機制，透過區塊鏈技術結合多元應用系統之個人帳戶身分識別，用來綁定自然人憑證與多元應用服務管道之個人身分資料，以期將來只需要擁有自然人憑證即可登入、操作多個應用系統。

（五）結合自然人憑證提供應用服務的個人身分資料存證功能



提供各項應用服務自然人憑證簽驗章功能，針對不同的應用服務只要透過本系統提供的個人身分資料存證 API，使用者須持自然人憑證，根據多元應用服務管道將打包過後的個人身分資料進行簽章作業，並將這些個別應用服務管道之個人身分資料雜湊值(hash value)及該雜湊值的簽章值(signature value)透過智能合約存證於區塊鏈中。並提供區塊鏈申辦應用於內政部各類申請案件之身分識別機制，如下圖



智能合約(Smart Contract)是區塊鏈中一種制訂合約時所使用的協議，主要用於提供自動化執行驗證及智能合約內所訂定的條件，包括互動、做決策、儲存資料…等功能，本機制將會開發以儲存資料功能為主的智能合約，開發各應用服務通用的智能合約樣板，存儲打包過後的個人帳號資料及簽章資訊，

透過本機制提供一個具有可追蹤、難以竄改與不可逆的儲存與驗證服務。

進行驗證服務時，應用服務會先透過本系統提供的個人身分識別 API，經由智能合約從區塊鏈中取出打包過後的個人身分資料(hash value)及該打包後個人身分資料的簽章值(signature value)，使用者須持自然人憑證對從區塊鏈取出的資料進行驗簽章作業，若能通過簽章驗證程序，證明打包過後的個人身分資料確實與該自然人憑證綁定，則認可該應用服務所屬之個人資料與該自然人憑證的身分為同一人。

六、研究 ECC 及後量子密碼學

目前全世界已有包含捷克、德國、立陶宛、拉托維亞、俄羅斯、阿拉伯聯合大公園、塞普露斯、比利時等國使用 ECC 演算法於 eID/ePassport 中，而對於我國未來國民身分識別證裡也可能包含使用的 ECC 金鑰，故我們預計研發提供 ECC 相關功能服務。

（一）對於我國未來國民身分識別證裡也可能使用的 ECC 金鑰，我們預計將能提供絕大部分與目前 RSA 金鑰相同的功能作業，例如：使用 ECC 金鑰進行憑證申請、廢止、停復用、展期等。

(二) 對於原 MOICA 系統來說，為了降低衝擊及增加相容性，我們將研究規劃另建一 ECC 金鑰的憑證信任鏈，可與目前 RSA 金鑰為主的憑證信任鏈並存。

(三) 當用戶要使用 ECC 金鑰相關的憑證功能服務時，我們系統將使用前述新建 ECC 金鑰的憑證信任鏈為基礎來提供相對應的服務。

(四) 研究國際 PQC 密碼學最新候選標準，對 NIST 制訂標準過程分階段釋出的各候選演算法進行了解、測試和掌握。

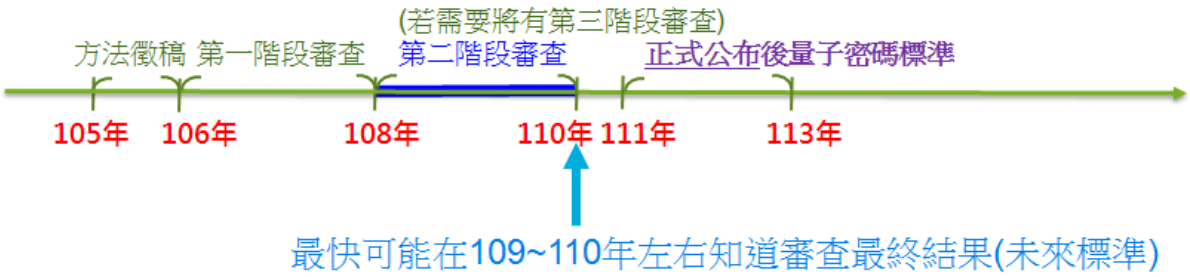
目前現有絕大多數公鑰密碼演算法（RSA、Diffie-Hellman、ECC 等）能被足夠大和穩定的量子計算機破解，如下表所示。

Cryptosystem	Broken by Quantum Algorithms?
RSA public key encryption	Broken
Diffie-Hellman key-exchange	Broken
Elliptic curve cryptography	Broken
Buchmann-Williams key-exchange	Broken
Algebraically Homomorphic	Broken
McEliece public key encryption	Not broken yet
NTRU public key encryption	Not broken yet
Lattice-based public key encryption	Not broken yet

其中，根據估計，破解基本的RSA 1024需至少5000qbit(量子位元)的量子電腦，但量子電腦近年快速發展，產業界目前已有數十到近百 qbit 的量子電腦(IBM, Google, Intel)，不過產業界猜測美國私底下可能已有數百個 qbit 的量子電腦，甚至產業界也認為從數百到數千 qbit 的進展可能很快。

針對目前量子計算破解密碼系統的能力來說，非對稱式/公鑰密碼系統(例如 RSA、ECC)會被量子計算演算法 Shor algorithm 所破解，而對稱密碼系統(例如 AES、DES)則會被量子計算演算法 Grover algorithm 破解；對於防禦量子計算破密方法來說，以目前已知的量子電腦能力而言，公鑰密碼系統需更換底層密碼學方法，也就是將 RSA 和 ECC 密碼學方法改用 PQC 後量子密碼學方法，而對稱密碼系統只需做強化即可，例如將 AES 金鑰長度加倍(如使用 AES-256)，故對整體密碼相關系統來說，非對稱式/公鑰密碼系統(例如 RSA、ECC)受到的衝擊最大，必須要換掉演算法才能解決量子電腦威脅問題。

美國 NIST 目前正進行此下一代公鑰標準 PQC 後量子密碼標準之篩選作業，期程如下，最快可能在未來兩年確認審查結果(未來標準)，最晚會在111年至113年對外公佈 PQC 最終標準演算法。



由於 NIST 表示由於量子電腦未來破密能力可能超過目前的預

估，故 NIST 將不會「把雞蛋放在同一個籃子裡」，此次 PQC 密碼最新標準很可能一反常態，不會推出單一密碼學演算法作為最終標準，而是會推出多個基植於不同數學難題的密碼學演算法，以避免當未來量子電腦又繼續攻破其中某個數學難題領域後，還有其他的選擇可使用。由於本次 PQC 候選演算法跨越的數學領域非常大，每個候選演算法的特性和適用情境皆非常不同(金鑰長度、簽章大小及簽章/驗簽章速度、密文長度及加密/解密速度)，且大部分演算法的上述性質都很可能超過目前電腦及網路環境用戶能容忍及負荷的範圍，故非常有必要先行了解、評估相關的衝擊，並即早做先期的規劃準備及配套措施。

以目前 NIST 公布的 PQC 標準的候選演算法來說，可抵抗量子計算的後量子密碼有以下方法，並且依照 NIST 說法，很可能每個領域都會選出一代表該領域數學難題的 PQC 標準演算法：

- 編碼密碼學 (Code-based cryptography)
- 雜湊密碼學 (Hash-based cryptography)
- 網格密碼學 (Lattice-based cryptography)
- 多變量密碼學 (Multivariate cryptography)
- 超奇異橢圓曲線同源密碼學 (Supersingular elliptic curve isogeny cryptography)

(五) 研發基於最終版 PQC 標準之 PQC 系統服務

我們將針對國內自然人憑證應用情境和環境需求，在可能的多種 PQC 密碼最終標準中選出最適合的演算法。

如前面所述，依照 NIST 說法，很可能每個領域都會選出一代表該領域數學難題的 PQC 標準演算法，但其實這幾個不同領域的 PQC 演算法在功能性上並不完全相同，如下表所示。

	加解密	簽章	金鑰建立方式	
			Key Transport	Key Agreement
Code-based	√	√	√	×
Hash-based	×	√	×	×
Lattice-based	√	√	√	√
Multivariate	√	√	√	×
Supersingular	√	√	√	√

而且這幾個不同領域的 PQC 演算法在簽章等功能的效能表現上也不相同，並且相較傳統密碼學(RSA,ECC)，後量子密碼學(PQC)的缺點包括金鑰、簽章的 size 較大 (下圖是各演算法的平均長度比較)，因前述 size 問題，運算速度也較慢。

	公鑰+簽章長度(KB)
ECDSA	∼ 0.1
RSA	∼ 0.5
Stateful HBS	15
Stateless HBS	42
Code-based	190
Lattice-based	11
Multivariate	99
SS Isogenies	122

由以上可知，大部分後量子密碼學的金鑰及簽章長度，還有運算速度，會較傳統密碼學方法來的差。但本次美國國家標準局 NIST 即是透過徵選的方式，就是要找出能夠克服以上效能問題的新的後量子密碼學演算法，例如其中的 Lattice-based 方法就被認為在改進後很有可

能效能表現能與傳統密碼學(RSA、ECC)差距縮小許多。

在系統研發方面，我們對於未來 PQC 系統服務由於要處理較長金鑰及簽章長度、運算速度慢等效能問題，到時要如何從目前傳統公鑰密碼系統要轉移至後量子密碼系統會是一個重要問題。

因此，Crypto-agility (cryptographic agility) 是除了後量子密碼學演算法的制定外，另一個 PKI 系統應該關切的研究項目。

Crypto-agility 使得資訊安全系統可以轉移至其他密碼學元素或演算法而不需要重大的改變系統基礎，因而有助於促進資訊系統升級與發展。當資訊系統被發現其密碼學演算法可能有缺陷時，Crypto-agility 可以作為安全措施或立即反應機制。若該系統之密碼學演算法可以被容易地更換且至少有部分自動化，則可被認為 Crypto-agility。

對現行 PKI 系統而言，最重要就是要在事前逐步移轉至後量子演算法的協定和格式。

Crypto-Agility PKI 系統未來需要討論的議題包括以下：

- 演算法的自動調整：
  - SSL/TLS 等協定需要可以依據雙方支援程度調整演算法
  - 各種加密或簽章格式須能同時兼容多種演算法
- 憑證格式相容：
  - 需要能夠同時相容傳統與後量子密碼學之公開金鑰和簽章
  - 既有應用系統無須更新亦能如常使用才能順利大量推廣

因此，我們將對國內自然人憑證應用和環境需求進行分析，針對上述議題找出最好的解決方法，以提供 PQC 後量子密碼系統服務，對量子電腦此類國家級安全威脅提供最佳的安全防護。

七、應用推廣

（一）提供對外介接函示庫及網頁認證介接服務。

（二）辦理教育訓練及大型說明會。

肆、 主要工作項目與辦理時程（110-114年度）

一、110-111年：自然人憑證行動化及 AI 智慧客服與電子報簡訊平台整合客戶管理平台

(一) AI 智慧客服平台建置

1. 服務水準制訂
2. 資安政策擬定及資安防護
3. 平台設計開發建置
4. 大數據資料庫建置
5. 整合客戶管理系統
6. 維運及客服人員席次增加
7. 整合內政部超商 KIOSK 服務平台

(二) AI 電子報簡訊平台整合客戶管理系統

1. 服務水準制訂
2. 資安政策擬定及資安防護
3. 平台設計開發建置
4. 設計開發用戶端通知軟體

(三) 內容傳遞網路 CDN 空間租用

空間租用及網路設定

(四) 行動化憑證平台

1. 資安政策擬定及資安防護
2. 平台設計開發建置
3. 憑證註冊窗口建置
4. 整合至客戶管理系統

二、112-113年：多元及區塊鏈身分識別

(一) 區塊鏈多元身分識別平台建置

1. 資安政策擬定及資安防護

2. 建置區塊鏈身分識別服務系統

3. 介接 T-ROAD 或各單位 LDAP 服務，以擷取用戶個人資料

4. 結合自然人憑證提供申辦應用服務的個人身分資料記錄功能

5. 提供區塊鏈內政部各類申辦身分識別及交易紀錄

6. 整合至客戶管理系統

三、114年：系統營運及未來研究發展

(一) AI 智慧客服平台系統維運

1. 設備及資料維護作業

2. 功能增修及資安修補作業

3. 服務滿意度調查

(二) 區塊鏈多元身分識別平台系統維運

1. 設備及資料維護作業

2. 功能增修及資安修補作業

3. 服務滿意度調查

(三) 研究發展

1. 金鑰風險評估及憑證展期可行性研究

2. ECC 憑證發證可行性研究

3. 後量子密碼學研究

(四) 應用推廣

1. 函示庫更新

2. 教育訓練

3. 說明會

伍、 資源需求（110-114年度）

一、 計畫專案人力需求

本計畫並無編列人事相關費用，計畫之整體規劃與執行將由內政部既有人力組成專案小組統籌辦理，並依據「行政院所屬各機關資訊業務委外服務作業參考原則」，基於提升營運效率之考量及在能夠有效監督、評估及控制委外服務品質之前提下，將後續細部規劃、設計、監造及建置委外辦理。

人力及資源請參考附件

單位：人/年 (人/月)

計畫名稱	110年度							111年度	112年度	113年度	114年度
	總人力	人員類別						總人力	總人力	總人力	總人力
		專案管理師	資訊系統分析及設計師	軟體發展及程式設計師	資料庫及網路專業人員	平面及多媒體設計師	其他文人(含書資料輸入員)				
自然人憑證多元身分識別服務計畫	18.92 (227)	2.58 (31)	4 (48)	4.92 (59)	4.42 (53)	1 (12)	2 (24)	18.92 (227)	19.92 (239)	18.25 (219)	15.17 (182)

註一：請填入預計由計畫支薪之計畫執行人員。

註二：本年度填「申請人力」，過去年度填「實際人力」，核定或執行中者填「核定人力」，預核年度填「預估人力」。

註三：職級(分6級)

1. 研究員級：研究員、教授、主治醫師、簡任技正、若非以上職稱則相當於博士滿三年、或碩士滿六年、或學士滿九年之研究經驗者。
2. 副研究員級：副研究員、副教授、助研究員、助教授、總醫師、薦任技正、若非以上職稱則相當於博士、或碩士滿三年、學士滿六年以上之研究經驗者。
3. 助理研究員級：助理研究員、講師、住院醫師、技士、若非以上職稱則相當於碩士、或學士滿三年以上之研究經驗者。
4. 研究助理級：研究助理、助教、實習醫師、若非以上職稱則相當於學士、或專科滿三年以上之研究經驗者。

5. 技術人員：指目前在研究人員之監督下從事與研究發展有關之技術性工作，且具備下列資格之一者屬之：初(國)中、高中(職)、大專以上畢業者，或專科畢業目前從事研究發展，經驗未滿三年者。
6. 其他：指在研究發展執行部門參與研究發展有關之事務性及雜項工作者，如人事、會計、秘書、事務人員及維修、機電人員等。

註四：當年度應填列詳細資料(含研究員級以上、副研究員級、助理研究員級、研究助理級、技術人員等)。

二、各工作項目及其經資門需求　　單位：千元

工作項目		110 年	111 年	112 年	113 年	114 年	合計
服務水準暨資安防護政策	經常門	2,500	0	1,600	0	0	4,100
	資本門	0	0	0	0	0	0
AI 智慧客服平台建置	經常門	13,550	13,016	3,228	3,228	3,228	36,250
	資本門	3,190	2,524	0	0	0	5,714
大數據資料庫建置	經常門	8,200	8,200	2,000	2,000	2,000	22,400
	資本門	1,800	1,800	0	0	0	3,600
客戶管理系統	經常門	5,050	8,740	2,090	2,090	2,090	20,060
	資本門	990	1,800	0	0	0	2,790
行動化憑證平台	經常門	4,920	4,920	1,200	1,200	1,200	13,440
	資本門	1,080	1,080	0	0	0	2,160
超商服務平台整合	經常門	2,050	2,050	0	0	0	4,100
	資本門	450	450	0	0	0	900
用戶端通知軟體	經常門	4,100	3,444	920	920	920	10,304
	資本門	900	756	0	0	0	1,656
多元及區塊鍊身分識別平台建置	經常門	0	0	11,132	7,652	3,108	21,892
	資本門	0	0	6,610	7,690	0	14,300
屬性憑證	經常門	0	0	3,000	0	0	3,000
	資本門	0	0	0	0	0	0
註冊窗口集中化	經常門	0	0	8,200	1,000	1,000	10,200
	資本門	0	0	1,800	0	0	1,800
函式庫整合	經常門	0	0	0	3,280	0	3,280
	資本門	0	0	0	720	3,000	3,720
強化電子化政府應用、擴大開放應用	經常門	0	0	2,000	14,000	27,233	43,233
	資本門	0	0	0	0	0	0
軟硬體設備擴充	經常門	0	0	0	0	0	0
	資本門	5,000	5,000	5,000	5,000	5,000	25,000
研究發展及應用推廣、政策宣導	經常門	2,000	2,000	7,000	7,000	7,000	25,000
	資本門	0	0	0	0	0	0
總計		55,780	55,780	55,780	55,780	55,780	55,780

陸、 預期效益分析

一、 強化自然人憑證便民服務減少民怨

(一)有效處理民眾客訴減少客訴數量

(二)降低民眾客訴處理時間

二、 多元便民服務管道

(一)文字化 AI 客服介面，不論 PC 或行動裝置皆可使用

(二)超商提供卡片是否損壞判讀及使用用戶代碼解鎖卡或用戶代碼重置 24 小時便民服務

三、 增加應用廣度及深度

(一)自然人憑證行動化結合本部各類電子申辦，方便民眾直接申辦及查詢進度

(二)自然人憑證行動化結合各類網路行動化申辦需求

柒、 關鍵績效指標設定及衡量基準(請各工作項目至少填列1項指標)

計畫目標	績效指標	評估方式	衡量標準	指標值				
				110年	111年	112年	113年	114年
憑證使用度	自然人憑證使用量	使用人次	超過8000萬人次/年	8000萬	8500萬	9000萬	9500萬	10,000萬

捌、 前期或相關計畫之過去成果、績效及決算情形

年度	相關計畫名稱	法定預算數（千元）	決算數（千元）	簡要說明(過去成果、績效)
108	內政多元憑證創新計畫	43,634	43,634（預估）	1. 自然人憑證發證量105年約43.7萬張，106年48.6萬張，107年52.1萬張，平均每年達9.7%成長，截至108年12月15日止總累計發證量達705.4多萬張。 2. 截至108年12月底止總累計已超過10.52億人次上網應用自然人憑證，若以每次可節省民眾100元相關費用計，共可至少節省民眾約1052億元，顯示成效頗佳。

玖、 資安與個資風險評估及資安防護機制

一、 界定個人資料使用範圍

二、 個人資料之風險評估及管理規範制定

三、 事故之預防、通報及應變機制

四、 個人資料蒐集、處理及利用之內部管理程序制定

五、 資料安全管理及人員管理計畫

六、 設備安全管理計畫

七、 資料安全稽核機制

八、 使用紀錄、軌跡資料及證據保存

壹拾、 遭遇問題及因應對策

一、預期遭遇困難

（一）系統效能不佳，網路頻寬及硬體處理資源不足。

（二）投入客服勞務人力不足，無法有效降低客訴量。

（三）機關應用個人化識別個別需求。

二、因應對策

（一）緊急採購硬體資源，及擴充網路頻寬。

（二）緊急調度客服勞務人力大量投入。

（三）規劃建置區塊鏈多元身分識別平台

壹拾壹、資安經費投入自評表

部會			單位				
審議編號	計畫名稱	期程(年)	總經費(千元)(A)	資訊總經費(千元)(B)	資安經費(千元)(C)	比例[註1](D)	備註
	自然人憑證創新應用服務	5	278,900	255,200	23,700	8.5%	

資安經費投入項目				
項次	年度	投入項目類別[註2]	投入項目	預估經費（千元）
1	110-114	A1	依據資通安全管理法—資通安全責任等級分級辦法之「資通系統防護需求分級原則」，完備「資通系統防護基準」之各項措施	15,000
2	110-114	B1	依據資通安全管理法—資通安全責任等級之公務機關應辦事項，建置必要之縱深防禦機制，含網路層(例如：防火牆、網站防火牆等)、主機層(例如：防毒軟體、電子郵件過濾機制等)、應用系統層等資安防護措施	6,200
3	110-114	B3	各項設備應導入政府組態基準(Government Configuration Baseline，GCB)	2,500
總計				23,700

備註：

1、 資安經費提撥比例係依計畫總經費(A)或資訊總經費(B)計算(可多計畫合併)，各計畫可依業務性質及實際需求於計畫執行年度分階段辦理。

1.1 109年(含)前結束之計畫，其需達成資安經費比例(D)計算方式=(資安總經費(C)/資訊總經費(B))*100%，1億(含)以下提撥7%、1億以上至10億(含)提撥6%、10億以上提撥5%。

1.2 110-114年(含)後結束之計畫，除前述資安經費比例，另配合行政院政策逐年提高資安經費比例至「資安產業發展行動計畫(107-114年)」所訂114年預期達成目標。

2、 投入項目類別請用下列代號填寫：

2-1 系統開發

(A1) **依據資通安全管理法-資通安全責任等級分級辦法之**「資通系統防護需求分級原則」，完備「資通系統防護基準」之**各項措施。**

(A2) 推動「安全軟體發展生命週期(SSDLC)」，可參考行政院國家資通安全會報技術服務中心所訂「資訊系統委外開發 RFP 資安需求範本」。

(A3) 依據經濟部工業局所訂「行動應用 APP 安全開發指引」、「行動應用 APP 基本資安檢測基準」、「行動應用 APP 基本資安自主檢測推動制度」等，進行相關資安檢測作業。

2-2 軟硬體採購

(B1) **依據資通安全管理法–資通安全責任等級之公務機關應辦事項，建置必要之縱深防禦機制，含網路層(例如：防火牆、網站防火牆等)、主機層(例如：防毒軟體、電子郵件過濾機制等)、應用系統層等資安防護措施。**

(B2) **推動國內認證/驗證規範，並將該產品通過之相關認證/驗證或符合相關規範納入建議書徵求說明書，例如：影像監控系統需符合影像監控系統相關資安標準，且經合格實驗室認證通過。**

(B3) **各項設備應導入政府組態基準(Government Configuration Baseline，GCB)。**

2-3 其他建議項目

(C1) 資安檢測標準研訂。

(C2) 新興資安領域(例如：5+2產業創新計畫)之資安風險與防護需求研究。

(C3) 新興資安領域之人才培育。

(C4) 編撰資安訓練教材。

(C5) 其他資安相關項目(例如：推動「資安產業發展行動計畫」之四項策略-建立以需求導向之資安人才培訓體系、聚焦利基市場橋接國際夥伴、建置產品淬煉場域提供產業進軍國際所需實績、活絡資安投資市場全力拓銷國際)。