



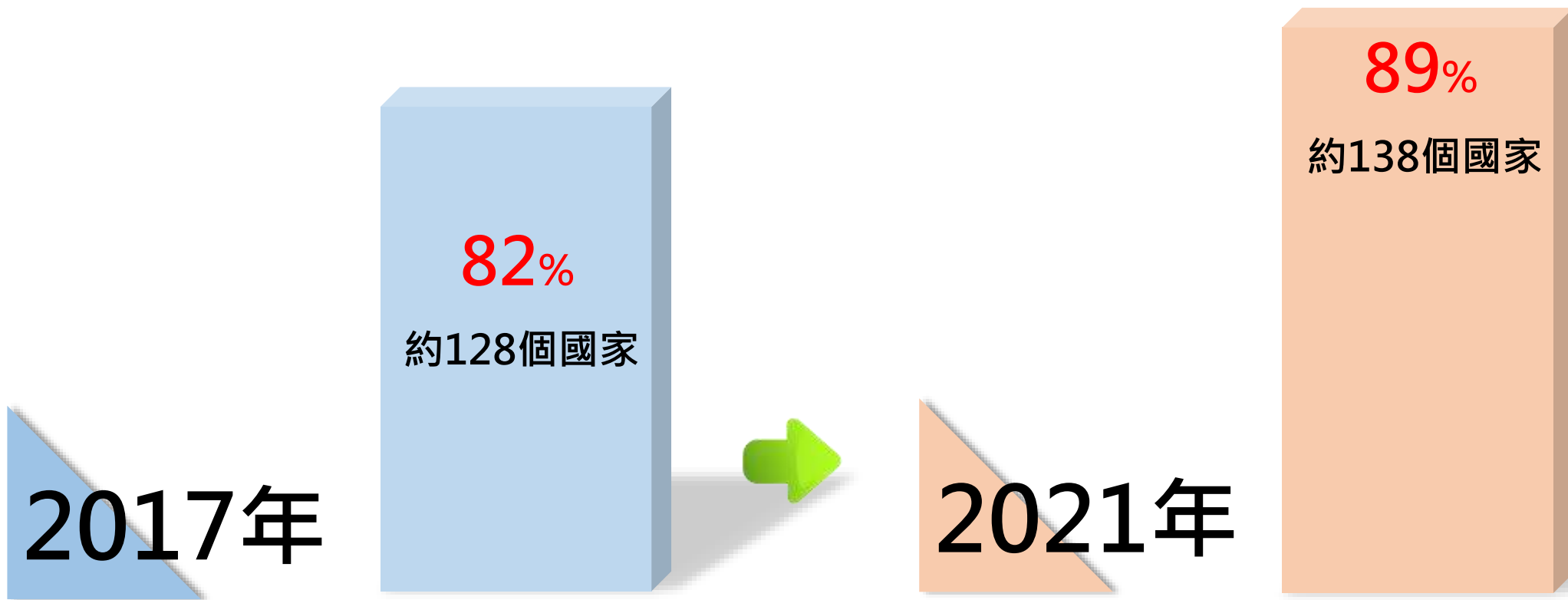
數位身分識別證 說明簡報

109年11月

New eID



▶ eID是世界潮流趨勢



全球發行國家身分證明文件者，採用晶片卡之比例

特色



(1) 嚴謹綁定身分

須至戶所臨櫃領取



(2) 普及全國

全國普發，每位國民都有



(3) 身分識別最高等級

符合**數位身分驗證等級4**
(Level of Assurance, LoA)



(4) 數位簽章最安全

確保線上交易完整性與不可否認性



➤ 各機關得於使用New eID身分識別後，再自行建立認證管理機制。

ISO 29115 「數位身分驗證等級」



國際標準化組織, ISO

(International Organization for Standardization)

強化防偽

PC

耐用 **10年**

多層融合 不剝落褪色

雷射雕刻 個人資料

多數國家採用(已發行eID者)

- ◆ 高解析彩色相片
- ◆ 高端防偽變造技術

透明視窗 光影變化箔膜 (OVD) 多重雷射影像.....

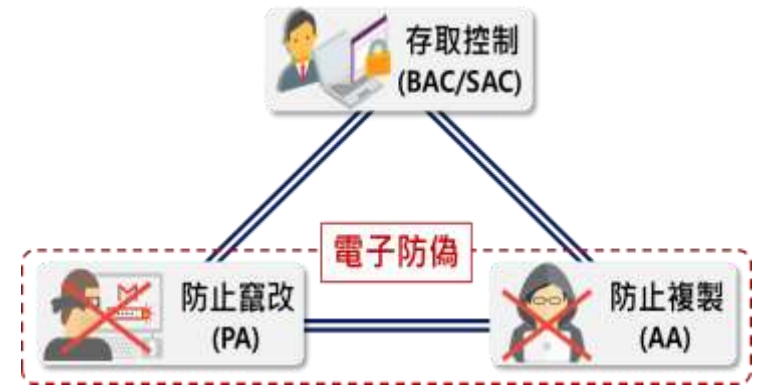


雙重防偽

- ◆ 封裝後無法取出
- ◆ 無法被側錄



- 建立一次性安全通道傳遞資料
- 動態產生金鑰進行資料加密
- 晶片卡移除後，清除所有內容及通道



- ◆ 無法複製偽造

讀卡機是否有惡意元件屬
應用機關資安檢測項目

卡面個資最小化



正面欄位資訊

1. 姓名
2. 統一編號
3. 出生日期
4. 相片



背面欄位資訊

1. 結婚狀態
2. 製證日期
3. 應換領日期
4. 卡片序號條碼
5. 統一編號條碼
6. 機讀區(MRZ)

現行



卡面個資過多



紙本揭露 11 項個資

未來



卡面個資 5 項

晶片內個人資料分區保護

晶片個人資料不多於紙本身分證

雙介面(插卡&感應)讀取

1. 戶籍地區

1. 戶籍地址
(僅到村里鄰)

◎無個人資料，可直接讀取

2. 公開區

1. 姓名
2. 統一編號
3. 出生日期
4. 戶籍地址
5. 役別
6. 結婚狀態
7. 相片(300dpi)

◎輸入**讀取碼**才可讀取

讀取碼：卡片序號後6碼
或機讀碼

僅得插卡讀取，無法感應讀取

3. 加密區

1. 配偶姓名
2. 父姓名
3. 母姓名
4. 出生地
5. 性別

+ 公開區資料

◎需用機關須經本部同意，由本人輸入**密碼**才可讀取

密碼(PIN1)：自訂 6 位數字

4. 自然人憑證區

1. 姓名
2. 統一編號後4碼

自主選擇是否附加
(已附加者，日後可申請停
(復)用或廢止)

◎由本人輸入**憑證密碼**才可使用

憑證密碼(PIN2)：自訂 8~12 位數字

連錯3次自動鎖卡

隱私資料加密保護

- 採eMRTD(電子機讀文件)檢查，啟用**非對稱式金鑰**防拷貝技術

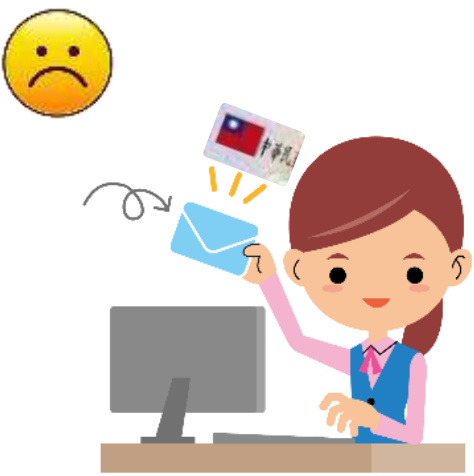
授權憑證控管

- 服務提供者(如公務、金融及醫院...)須向本部申請授權，始得讀取加密區資料
- 本部依服務提供者依法執行業務之需求，發給授權憑證，控管可讀取之特定欄位

✓ 各機關可透過每日提供之廢止清單或線上查詢確認卡片、自然人憑證有效性，讓保護更即時、更安全

尊重資訊自主

現行



個人資料都露

(申辦有線電視、租車)

未來



民眾選擇是否提供，不得強制讀取



OR



不願晶片被讀取者提供晶片資料清單
效力等同
電子戶籍謄本

國民身分證晶片資料清單
作為晶片資料紙本證明文件
(須搭配New eID使用)



民眾自己選擇是否附加自然人憑證功能
已申請者，可隨時申請停(復)用或廢止



OR



New eID...



跳出提醒視窗

*建議使用安全電腦及環境

數位身分識別證個人資料查詢及列印

數位身分識別證專區



登入後
可檢視個人分區資料及憑證資訊



國民身分證
晶片資料清單



介紹說明



申請、應用



常見問答集



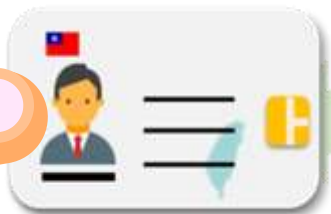
- 公開區 - 輸入讀取碼即可讀取
- 加密區 - 自訂密碼(PIN1)
- 憑證區 - 自訂憑證密碼(PIN2)

- 需設定密碼後才可以啟用
- 請勿用生日或身分證字號設定密碼

無國家監控



沒有一個機關可全然掌握
New eID 之使用軌跡



A 機關

B 機構

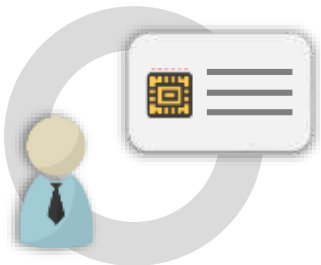
C 單位



不須連線
內政部



1. New eID若附加**自然人憑證**可作網路身分識別
使用時跟自然人憑證一樣，不會在憑證中心留下任何紀錄，由各服務提供者留存



2. New eID的**晶片存有個人身分基本資料**

辦理各項業務時，無須連回內政部取用個資，不會留下使用紀錄，更無從監控



每日更新公布
eID掛失資訊予
各機關



基本個資

- 免填寫
- 免登打



省力、省時



選擇附加自然人憑證者

- 免臨櫃
- 免奔波



省力、省時、省錢



換發New eID後





外部 5 層防護作業



防火牆(FW)、網路應用程式防火牆(WAF)
入侵偵測系統(IDS)、入侵防禦系統(IPS)
資訊安全監控中心(SOC)、戰情室

內部 4 層防護作業



資訊資產管理、防毒軟體
辦理日誌紀錄管理、資安內部稽核



委外廠商 4 層防護：

辦理廠商權限管控、維運連線側錄、
日誌紀錄管理、資安外部稽核作業



安全性檢測：

網站弱點掃描、滲透測試
資安健診

風險管控

安全標準

PC卡片 ISO/IEC 10373測試標準

- 晶片
- 接觸式介面：ISO 7816-3、T=1
 - 非接觸式介面：ISO 14443
 - 記憶體空間：144KB

晶片作業系統、資通產品

- 國際標準 Common Criteria
- ISO/IEC 15408驗證
- EAL 4+以上安全認證

資安管控



ISMS

資訊安全管理系統

(Information Security Management System)



IV&V

第三方獨立驗證及確認

(Independent Verification and Validation)

SOC

資安監控中心

(Security Operation Center)



集中製卡



提高製卡效率

提升資訊安全

增進卡片品質

降低發證成本



無法源
依據?

戶籍法、電子簽章法已有明定

戶籍法
第52條

國民身分證及戶口名簿之**格式**、**內容**、繳交之相片規格，由中央主管機關定之。

國民身分證及戶口名簿之**製發**、相片影像檔建置之內容、保管、利用、查驗**及其他應遵行事項之辦法**，由中央主管機關定之。

未逾越法律授權
不違反法律保留原則

因應數位化時代
智慧政府及網路行政服務



格式 紙本 ⇄ 晶片卡



內容 所載資料項目
(不超過紙本身身分證資料)

身分資料數位化
+
選擇附加自然人憑證

自然人憑證
發行依據

- 電子簽章法
- 內政部憑證管理中心憑證實務作業基準(CPS)

授權內政部

國民身分證全面換發辦法(109.3.19發布)

- ✓ 換證對象為在國內設有現戶戶籍之現住人口，不包括矯正機關收容人
- ✓ 領到通知單的民眾可以網路申請、排定地點申請、臨櫃申請、到府服務
- ✓ 本人親自領證，不可委託，未滿14歲由法定代理人陪同到場核對人貌並領取



109.9.2-11.2預告

「國民身分證及戶口名簿格式內容製發相片影像檔建置管理辦法」(109.12.25發布)

- ✓ 規定晶片儲存之資料項目，不得儲存非個人基本資料以外之資料
- ✓ 公開區或加密區資料，用於臨櫃之身分識別與資料驗證，及網路之資料驗證，不得作為網路之個人身分識別使用。
- ✓ 民眾設定晶片加密區及自然人憑證區密碼，並應妥善保管密碼
- ✓ 民眾可自行上網列印國民身分證晶片資料清單，配合國民身分證供需用機關查驗
- ✓ 晶片資料安全保護，除戶政機關無法變更
- ✓ 各資訊系統在儲存、傳輸或運用晶片資料時，應建立嚴密安全保護機制
- ✓ 執行業務時，查驗卡面資料即可辨識國民身分證真偽或個人身分，不得強制要求讀取晶片、機讀碼或卡片序號
- ✓ 讀取晶片加密區資料，應先經內政部授權，且須民眾輸入密碼
- ✓ 已核發之國民身分證，有事實足認晶片重大危害資通安全之虞時，應即啟動召回更換之機制，辦理資安通報及後續之換領或晶片韌體更新

至少要修法規範New eID內容及應用限制或立專法(比照德國)?



- 戶籍法第51條**效用及於全國**
- 戶籍法第56條國民身分證應隨身攜帶
→ **訓示規定無任何罰則**
- 「國民身分證及戶口名簿製發相片影像檔建置管理辦法」之修正，依行政程序法須預告
→ **行政機關無法任意修改擴權**
- 身分證之使用屬個人自由及相關服務提供之需要
→ **不宜於戶籍法規範**



德國身分證及電子識別法案計35條

15條規定

請領身分證條件、身分證記載項目、臨時身分證、身分證權責機關、身分證效力、沒收與繳回、費用、罰則等

- 戶籍法
- 國民身分證及戶口名簿製發相片影像檔建置管理辦法
- 內政部憑證管理中心憑證實務作業基準
- 戶政規費收費標準...

20條規定

晶片身分證之密碼、封鎖碼、解鎖碼、讀取碼及效期

「國民身分證及戶口名簿製發相片影像檔建置管理辦法」規範

錄存指紋

可取得晶片中生物特徵之機關

我國未錄存指紋及生物特徵

各國各有其法制體系，德國將eID相關規範集中在單一法律中，愛沙尼亞則是將相關身分證明文件集中在單一法律中，**我國係分別適用戶籍法、電子簽章法、資通安全管理法、個人資料保護法等規定**

舊證失效
有損權利?

各機關得視業務受理民眾以其他身分證明文件行使其權利

全面換證期間



全面換證結束



依戶籍法第59條第2項
規定公告舊證失效



可持新證行駛
各項權利義務

未換領新證者



- 得以其他身分證明文件，如中華民國護照、戶口名簿等，行使其權利。
- 如受行政機關不利益處分，而認其權利或法律上利益受有損害，可依法提起行政救濟。



立法明定
New eID應
用範圍？

由各機關依個別法令決定
須臨櫃親辦或線上服務項目



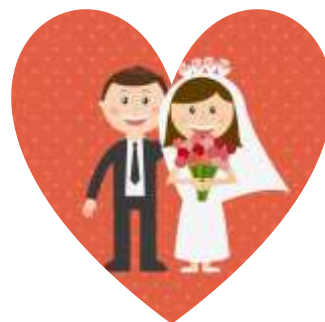
戶籍法第 51 條

國民身分證用以辨識個人身分，效用及於全國

線上服務
(由各機關提供)

臨櫃親辦
(依個別法令規定)

未來仍需親辦業務



結婚登記

結婚登記，以雙方當事人為申請人
(戶籍法第33條)



土地登記(委託他人)

登記義務人應親自到場，提出國民身分證正本 (土地登記規則第40條)



金融業務

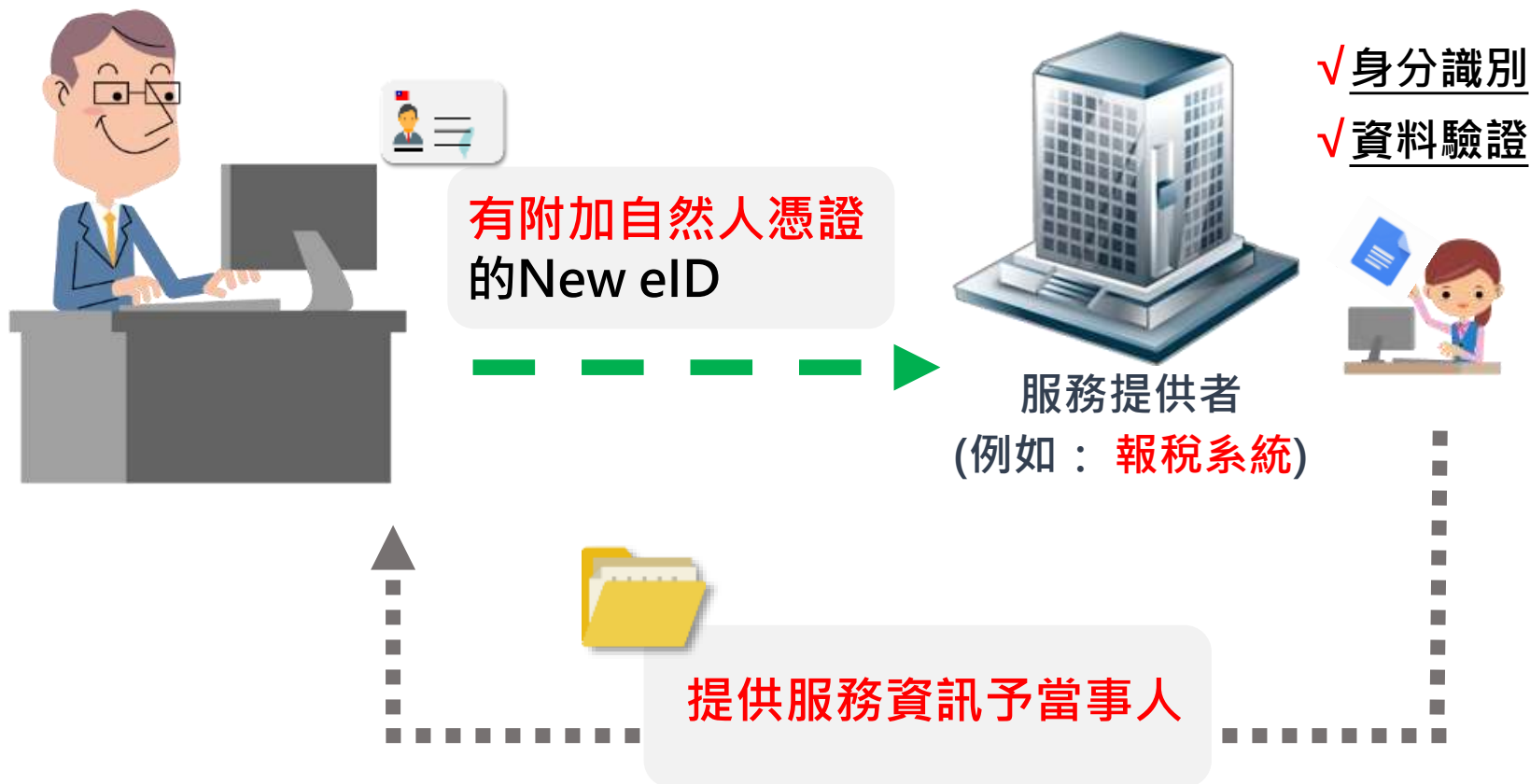
受理開戶時，應實施雙重身分證明文件查核及留存該身分證明文件
(金融機構防制洗錢辦法第3條)

可隨意進入
資料庫取用
個資？

各政府機關服務系統，可經由有附加自然人憑證的New eID
確認當事人身分後，提供所申請服務資訊予當事人

自然人憑證好處多：

可不用臨櫃，經線上識別身分後申辦健康存摺、報稅、戶籍謄本等業務，以及查詢監理車籍、財產總歸戶、勞保保費、有無限制出國等資訊...



以個資作為
網路身分認
證?

不附加自然人憑證的New eID僅能作為臨櫃身分識別及資料驗證，不能用於任何線上申辦之身分鑑別

不附加自然人憑證
的New eID

晶片公開區

晶片加密區



用於:

- 面對面身分識別及資料驗證，網路上的資料驗證
- 不得單獨作為網路身分識別及簽章
(須配套其他機制如需簽章則要當事人親簽文件才可為之)
- 不能用於任何線上申辦之身分鑑別

不要強制換發整合身分證及自然人憑證，最好兩卡分開？



讓人民有
選擇的權利

New eID
申請書

✗ 不申請
自然人憑證



戶籍地區

公開區

加密區

~~憑證區~~

- ❖ 不想使用憑證或晶片功能，使用上就如同現行紙本國民身分證一樣
- ❖ 國民身分證晶片資料清單搭配New eID作為身分證明文件

New eID
申請書

✓ 申請
自然人憑證



戶籍地區

公開區

加密區

憑證區

可自行決定
停(復)用或廢止



← 有需要者可自費再申請單張自然人憑證

原有自然人憑證效力？

已持有之自然人憑證，效期未至仍然有效



有效



有效



TIP

- ✓ 機關識別證與自然人憑證結合之職務憑證，仍可依現行方式發證
- ✓ 無論民眾是否選擇New eID附加自然人憑證，對於原已持有之自然人憑證，如效期未至，仍然有效。

不換New
eID不能投票？

全面換證期間，新舊證不影響投票權益

全面換證期間



無論是新證或舊證，民眾僅有一張身分證
均為有效身分證明文件，可持以投票

全面換證結束



65年：64/3 ~ 65/6
65年7月1日起失效

75年：75/3 ~ 12
76年1月1日起停止使用

94年：94/12~95/12/31
96年1月1日起停止使用

中國 管顧公司 規劃設計？

不允許大陸、含陸資成分及在臺陸資廠商參與

◇ 公司資格

- 國巨顧問公司**非大陸廠商**
- 依據公司登記資料，其股東均**與陸資無涉**

◇ 在地合作團隊

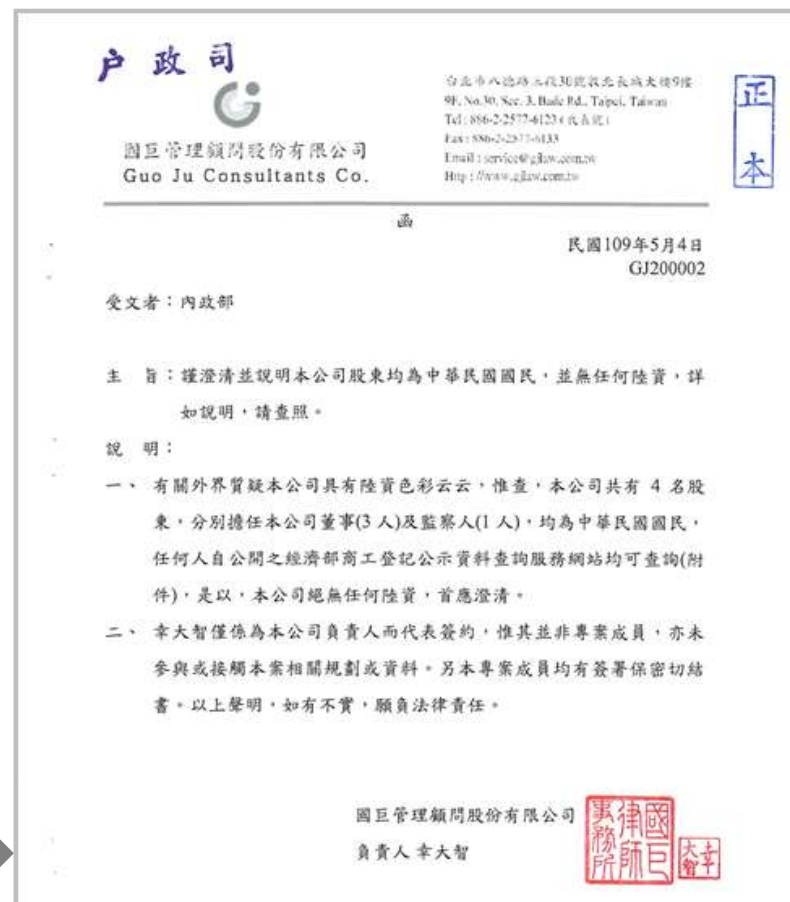
- 團隊係與工研院(巨量資訊科技中心)合作
- 團隊成員均簽有**保密切結**

◇ 該合夥人非本案成員

- 該公司合夥人**幸大智**具大陸律師證照並登記事務所，屬其個人業務
- **幸大智非本案成員無權知悉本案內容**

◇ 僅作規劃參考不參與建置

◇ 該公司已提具聲明書



工程會認定招標機關招標規範就國安、資安已有考量



- ✓ 不允許大陸地區廠商、第三地區含陸資成分廠商及在台陸資廠商參與。專案負責人及專案團隊不得為大陸地區人士。
- ✓ PC晶片卡(含晶片模組、作業系統及應用程序)及印製設備(含電腦設備軟硬體系統)之來源亦不可為中國大陸地區等規定。
- ✓ 國外卡廠IDEMIA(在捷克)僅負責空白卡製作，無個資寫入，無法接觸個資。
- ✓ 空白卡交付至中央印製廠後，進行晶片檢測、洗卡(自行產製具高度加密安全之新金鑰替換寫入晶片內)等安全管控作業並於網路封閉環境作業，不會發生晶片被植入惡意程式的風險。
- ✓ 專案成員皆簽署保密協定。

製卡招標
有弊？

經工程會確認，均符合政府採購法規定

東元電機

國內系統商
中華電信
(金鑰管理)

美國設備商
Entrust Datacard
(製卡設備)

國內卡廠
宏通數碼
(750萬PC空白卡)

國內卡廠
東元捷德
(750萬PC空白卡)

荷蘭晶片商
NXP
(台積電製造之晶片)

法國封裝廠
SPS
(晶片封裝)

捷克卡廠
IDEMIA
(1500萬PC空白卡)

德國卡廠
VERIDOS
(防偽元件)

依採購條款，國內廠商可單獨投標，
分包廠商家數以4家為限，國外廠商
亦可為分包廠商。

係分包不是轉包



國外卡廠
遭世界銀行
停權？

國外卡廠IDEMIA已澄清未遭世界銀行或其他多邊開發銀行停權，具備完整權限參與本案



- ✓ 國外卡廠 IDEMIA Identity & Security France S.A.S. (IDEMIA I&S) 僅製造無個人化PC卡。
- ✓ IDEMIA I&S，其捷克子公司或其任何相關聯公司，均無法接觸任何我國國人個資，個人化並不屬於IDEMIA I&S專案範圍的一部分。
- ✓ IDEMIA I&S目前沒有，在未來也不會由中國的製造工廠 IDEMIA (Shenzhen) Technologies Co., Ltd. 生產本專案PC卡。
- ✓ IDEMIA 集團係歐貝特科技(Oberthur Technologies)與賽峰身分與安全技術公司 (Safran Identity & Security, Morpho) 集團合併之事業；停權制裁僅影響曾屬於前歐貝特科技的IDEMIA 實體，而 IDEMIA I&S 並不在其中，IDEMIA I&S 未遭世界銀行或其他多邊開發銀行停權。

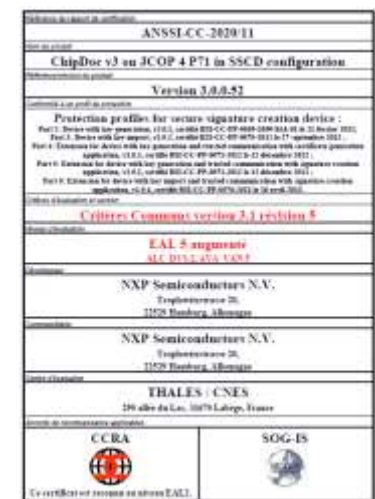
晶片規格 不安全？

高安全等級晶片 通過國際安全檢測

項目	高安全規格
晶片硬體、COS	確保非來自危害國家設計 原始碼經過國際專家檢視並通過CC認證
晶片Applet	原始碼經過國際專家檢視並通過CC認證
中介軟體 (公鑰加密標準-PKCS#11等)	提供原始碼及原始碼掃描報告

已通過 國際安全驗證之證書

CC認證：Common Criteria





恩智普(NXP)公司之晶圓
作業系統(COS)及應用程序(Applet)
於台積電晶圓製成時即已寫入，
避免被植入惡意程式

晶 片	認證等級
硬體架構	EAL 6+
密碼學函式庫	EAL 6+
作業系統	EAL 6+
應用程序 BAC	EAL 4+
應用程序 EAC+SAC	EAL 5+
應用程序 SSCD Part2+3	EAL 5+

EAL
5+

EAL 5+以上
軍事機密等級

CC認證(Common Criteria)之安全評估等級：
EAL (Evaluation Assurance Level，簡稱EAL)

★ 將再由國內專家進行資安掃描及檢核

項 目	資 安 檢 核
晶片Applet	提供完整的APDU規格書供第三方機構進行安全性檢視及分析
中介軟體 (PKCS#11等)	提供第三方機構進行安全性檢視及分析
客製化 客戶端軟體	由國內廠商開發並提供原始碼掃描報告 開放原始碼，供各界檢視安全性並提供修改建議

➤ Applet由NXP提供公版程式，並通過
CC認證以ROM燒錄，再由國內廠商做
資料與存取安全性設定

讀卡個資 被側錄?

晶片加密通道傳送個資



- ◆ 各業務系統讀取晶片時**建立資料傳輸安全通道**
- ◆ **安全通道為1次性使用**，每次加密通道金鑰不相同
- ◆ **無法側錄**傳送的資料

晶片安全機制

晶片對外通訊訊號
極微弱，**僅能在數
釐米內讀取**

輸入過強訊號，晶片
將啟動自動保護機制
而**自動關閉**



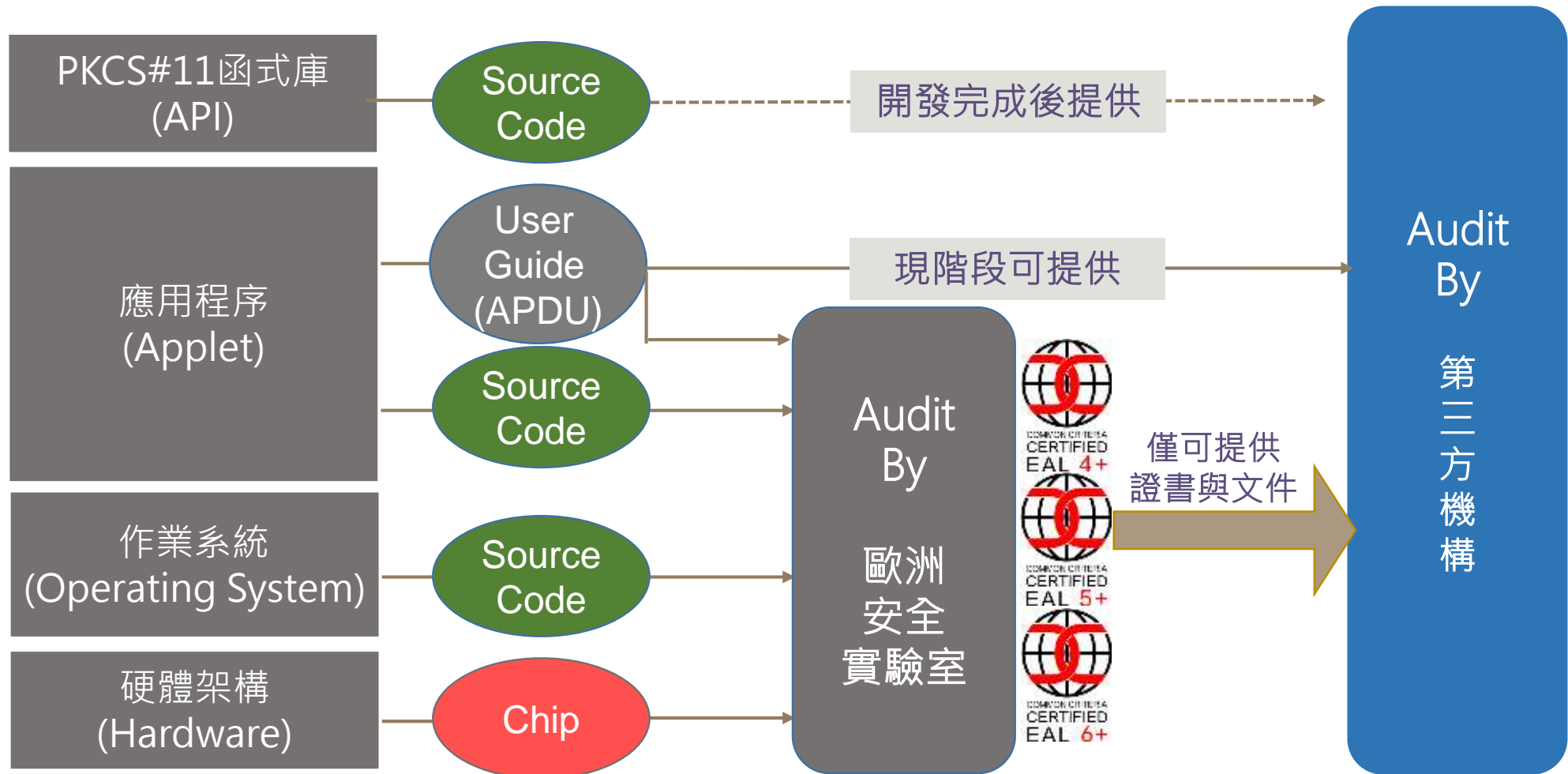
- ◆ 如使用非接觸式讀卡機，其感應距離係須為數釐米內

已請第三方機構出具卡片與讀卡機、卡片與API讀卡程式安全檢測報告

不公開
程式源碼？

公開程式源碼

核心程式交由第三方機構進行資安檢測



外商掌握系統建置?

透過管理面及技術面 層層嚴密管控系統建置廠商



管理面



技術面

- 簽署保密切結文件
- 監督與稽核：使用紀錄、軌跡資料之稽核、廠商內稽、機關及IV&V外稽
- 機敏資料讀取授權：限制行動化裝置使用、阻擋對外網路連線
- 廠商無高權限帳號：高權限帳號由機關控管
- 設備安全管理：委外作業人員之資訊設備均應受管理
- 門禁管理：進出本機關配帶臨時員工證件
非經許可不得至工作場所以外地區活動
- 處罰規範：違反規定，將依合約計罰
- 控管程式原始碼之存取權限：版本控制、源碼檢測
- 可控制開發環境測試與建置：整合式開發環境(IDE)
軟體開發套件(SDK)

外商掌握
製卡材料
及技術？

技術學習與移轉，整合國內晶片與資通訊廠商

因應作為

國內無PC晶片卡
與設備之產業鏈



臺灣生產製造

- PC晶片卡需有1,050萬張於臺灣生產製造或附加價值率超過35%
- 如印刷、燙印、鑲嵌天線、層壓融合、模切、植晶及金鑰對產製等製程

技術學習與移轉

- 提升國內製卡產業技術：透過與Idemia及Veridos 與 NXP合作
- 配合南向政策拓展東南亞證卡市場

培育潛在維運團隊能量

- 晶片產業鏈：晶片、卡片作業系統及Applet應用

個資保護
專責機構?



行政院
Executive Yuan

行政院研議中

- ◆ 專責機關成立前，各機關仍需依個資法使用、處理個資
- ◆ 管理或使用不當負損害賠償責任



直接
全面換發?

辦理小規模試行及賞金獵人競賽



試行
作業

- ◆ 規劃110年辦理試行推廣
- ◆ 由民眾自願申請New eID

賞金
獵人

- ◆ 辦理賞金獵人競賽
- ◆ 完備資安整備，再全面換證

New eID的規費規劃



補領
太貴?

強化不法風險管控，促使民眾妥善保管



雙重防偽



- ✓ 舊證換New eID及初領者**不收費**
- ✓ 為兼顧民眾負擔，暫定**換證收費300元**
 - 採晶片IC卡, 卡體防偽及晶片安全功能較高
 - 中央印製廠集中製證
 - 地方政府收件、審查發放、運送成本
- ✓ 為強化資安風險控管，規劃**補證收費900元**
 - 遺失涉及個人保管責任、不法風險等社會成本
 - 24小時受理掛失之值班人員人事成本及系統建置維護成本
 - 未滿14歲人晶片護照為900元，New eID之風險管控成本不宜低於護照
 - 強化民眾妥善保管意識，降低潛在不法風險

期程與經費

▶ 因疫情影響延遲，暫調整相關期程如下：



暫定期程

110年1月起

進行小規模試行由民眾自願申請New eID
辦理賞金獵人競賽

小規模試行
整備完善

開始啟動全面換發作業



預估經費

約 **48億元** (資訊安全總經費約為2億4仟萬元)

免收規費

- 全面換證期間
初領 & 持94年版舊證換領New eID者
- 全面換證期間結束
初領New eID者

New eID

Let's build the
future together!



邁入數位身分新紀元

New eID單純作為實體及網路世界中各項服務的身分識別，由政府所核發，具有公信力

普發**New eID**，全面建立安全可靠信賴的基礎環境

在這基礎之上產生強大的「**簡政**」、「**便民**」、「**創新產業增值應用**」、「**保護隱私、強化資安**」、「**尊重資訊自主**」的效果，能**與國際接軌**大幅提升國家競爭力！



New eID



簡報完畢