

妥善管理實體及行動憑證 打造全新服務樣貌

■作者：Michael Edwards

恩智浦半導體解決方案行銷部門總監

在此篇文章中，我們將檢視新興的憑證管理規則如何確保能正確的衍生及儲存憑證資料，以及介紹因使用衍生式憑證而受益的應用類型。我就從衍生數位憑證的最佳做法開始檢視。

eID 智慧卡打下良好基礎

若要順利轉移到數位存取，必須先以和智慧卡相關且經實證與認可的電子 ID(eID) 為基礎。這是因為 eID 智慧卡受到國家或國際標準規範的管理，技術方面也相當成熟，多年來用於數十億的身分驗證，無疑是深受信賴的身分識別方式。由 eID 智慧卡衍生的數位憑證，

顯示 eID 技術受到高度信任，能為數位行動裝置存取提供穩固基礎。

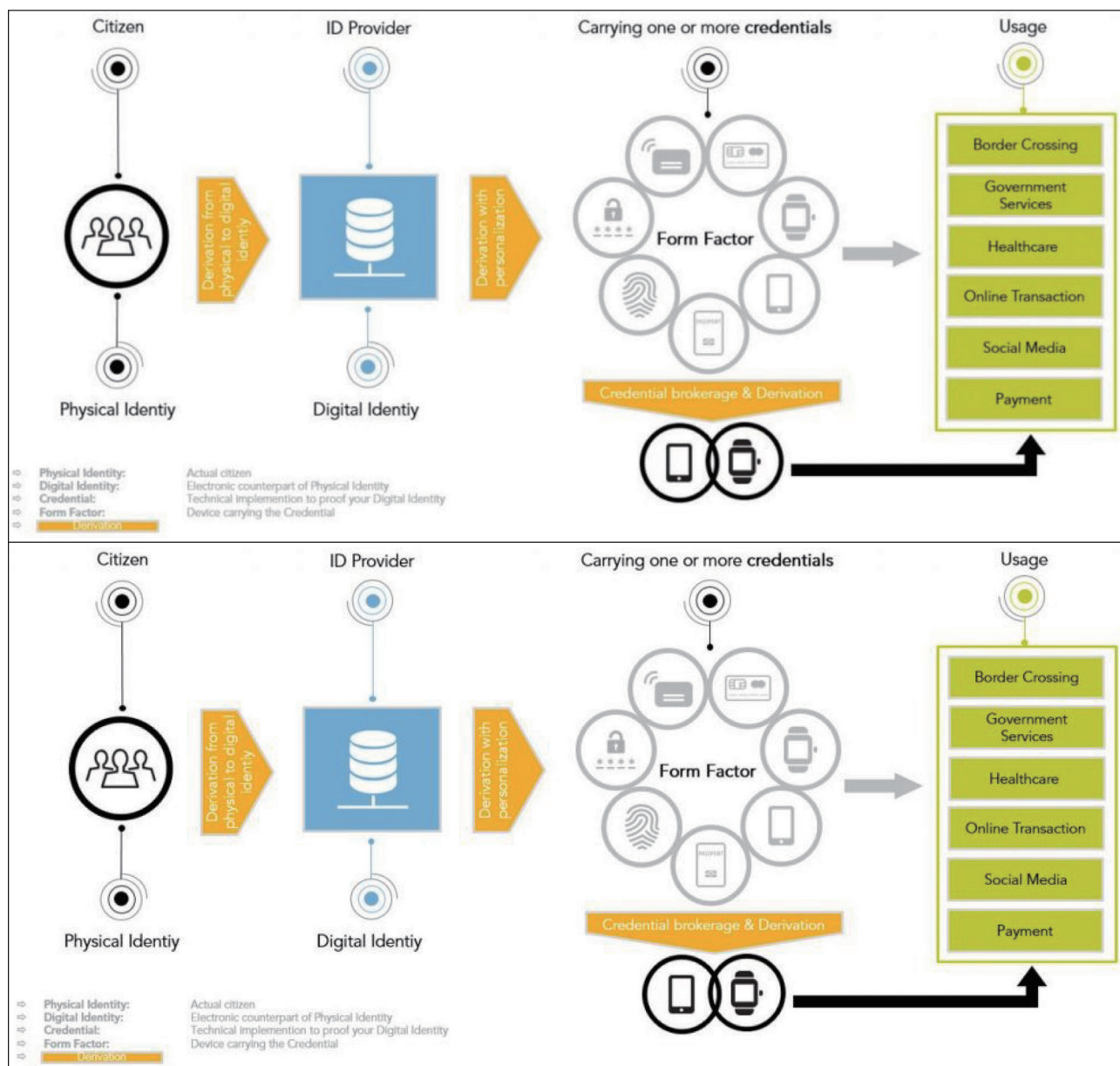
用來支援衍生式憑證的嵌入式安全元件 (embedded secure elements: eSE)，則是實現此項安全存取願景的另一重要因素，因為 eSE 能與現有非接觸式智慧卡的基礎架構相容 (包括使用 MIFARE 或 NFC 的架構)，而且能使用現有方法進行驗證。與現有基礎架構相容的內建功能，也有助於簡化部署並降低擁有成本。

若政府以衍生式憑證為基礎，建立一套備受信任的 ID 服務基礎架構，就能藉由新的基礎架構發行適用各種應用的單一 ID，進而更

接近從單一進入點存取多項服務的理想。用單一 ID 存取多項服務的模式，也稱做「同盟式」ID 管理，因為能安全使用私人數位資訊，同時能拓展服務範圍，因此也受到民間組織的推崇。

一個 ID，多種用途

舉例來說，要使用單一數位憑證來簡化多種服務存取，可以採用有包含兩種 Java 程序的智慧卡 eID 方案，而這兩種 Java 程序分別負責國民身分證與健保卡功能。但若要增加第三種駕照功能，智慧卡的設計就會變得更複雜，也需要更多利益關係人相互配合同意，才



能產生合適的卡片樣式。

不過，若有適當的衍生式憑證基礎架構並提供彈性的驗證平台，基本上就能消除這些設計限制。單一 ID 可以安全連結多種應用，進而運用於各種公共及私人服務。卡片一開始可以快速推行，之後再隨著時間增加新的使用案例。總擁有成本降低後，市民的選擇就增加了。

衍生式憑證的使用方式和傳統 ID 大致相同，差別在於衍生式憑證可用於行動環境中。以駕照為例，衍生式行動駕照可用來預約租車，並在操作車輛時驗證駕駛人的授權資料。國民身分證的衍生式憑證，則可在申請開立銀行帳戶、啓用新公寓設備服務、或加入當地圖書館時，作為居民認證。同樣地，健保卡的衍生式憑證可能用來驗證

醫療資訊，例如使用線上藥局或訂購眼鏡時，可以驗證藥物處方籤或矯正視力鏡片的資訊。衍生式憑證獨特結合了彈性與安全功能，因此能夠將任何公共或私人服務，轉移到行動裝置的操作環境。

情境感知驗證

現今許多線上應用程式的開發人員，常被迫在安全與便利之間

取舍。若是防護等級提高，驗證過程就會變得更複雜，因而降低使用的便利性。因此，若行動裝置能使用衍生式憑證，就無需的安全與便利之間取舍，因為行動裝置的格式能執行新世代的 ID 驗證方法，這種方法具有情境感知功能，既安全且容易使用。也就是說，後端系統使用的驗證方法會考量許多因素，例如：使用者是誰、使用者要求的服務、使用者的連線方式、當日時間、使用者所在位置等等。若是具備情境感知能力，驗證流程便能依照存取要求的來源，視其來自政府辦公室內部網路或公共 Wi-Fi，而使用不同的驗證規定。

這種情境感知方法能回應當前狀況而運作，因此能大幅提高安全性、便利性及成本效益。身分識別方法則可能因裝置與其特定功能而有所不同。例如，如果裝置配有

生物辨識感測器，能夠讀取指紋或辨識人臉或人聲，那麼就能採用生物辨識驗證法。如果裝置未配備生物辨識功能，則可以使用 PIN 碼、交易驗證碼 (TAN) 或密碼，作為驗證基礎。

衍生式憑證與情境感知驗證提高了應用彈性，因此更容易依照不同情況，選擇適當的安全層級。例如，存取醫療紀錄等高風險應用，可以使用多因素驗證 (multi-factor authentication) 來達到必要的安全等級，而風險較低的應用，則可以採用較不複雜的驗證方法，藉此降低技術成本而不危及個人隱私或安全性。

恩智浦因應 mGov 衍生式憑證的做法

憑藉數十年累積的技術經驗，

恩智浦在以 eSE 防護功能為基礎的安全服務領域中，更是知名的創新企業，日後會持續運用過往的寶貴經驗，打造適用其他行動裝置與 mGov 應用的解決方案。我們也建立強大的服務平台，為客戶帶來完善的數位驗證基礎架構，支援多種憑證類型。

恩智浦平台以 eID 硬體為起點，為行動應用程式的安全驗證服務，簡化設計與部署作業，並協助開發人員將多重應用 eID 作業，移植至行動裝置的應用環境。

若要深入瞭解相關解決方案，請造訪 (<https://www.nxp.com/applications/solutions/internet-of-things/secure-things/smart-government-identification:SMART-GOVERNANCE?&tid=vansmartgovernance>)。CTA

