Tokenization技術在不同產業的創新應用

撰文 | 叡揚資訊 資訊服務事業群、Gelmalto IDP亞太區高級資訊安全工程師 陳昶旭

若想要將重要資料去識別化，一般我們較熟悉的作法是透過加密，而由於個資保護議題興起，後來在部分應用領域當中，則實施遮罩。除了這兩者，現在我們還可使用資料記號化（Tokenization）或變造的方式來保護資料

蘋果與 Google 常有許多不同的理念，但面對行動支付安全保護信用卡資料一事，很難得地，同時指向 Tokenization 這項技術，好奇心驅駛我們一探這項異軍突起的技術，同時誘發我們思考在不同產業上的創新應用。

Masking、Tokenization 及 Encryption 之間的差異

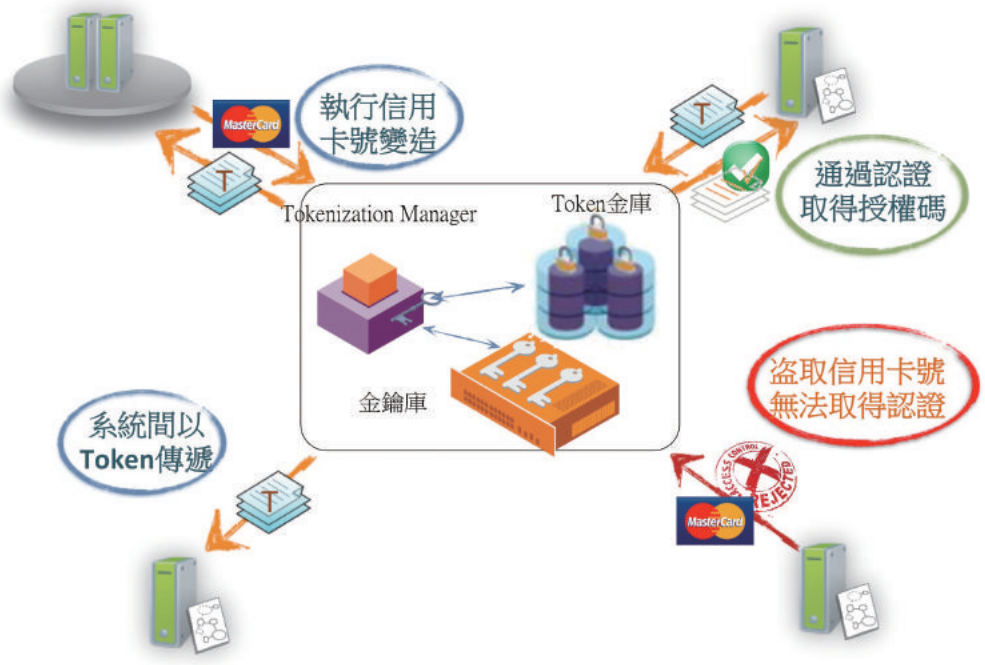
Masking（遮罩）、 Tokenization（記號化或變造）及Encryption（加密）觀念與應用，產生混淆。

- **Masking**：指對資料局部置換為特殊符號，如：○或※。
- **Tokenization**：將資料變化為另一組同性質資料，如：將身分證字號置換為另一組符合身分證字號編碼原則的字號，但不是真實資料。以目前來看， Masking 與 Tokenization 均為去識別化作法，並有逐漸合併趨勢。
- **Encryption**：指處理明文為亂碼型式的密文，如取得正確金鑰，可解密為明文，為可逆程序，通常密文長度會改變（也有密明文長度相同作法），通常密文不易對該單筆記錄追蹤分析運用，而執行 Tokenization 時，可運用雜湊金鑰，達到結果無法還原為原始資料，為不可逆程序，記號化資料可選擇不同方式呈現，如：保有原本長度，且可執行追蹤分析運用。

因此， Tokenization 、 Masking 及 Encryption 此三者之間，存在顯著不同。

↑一組信用卡號，經過記號化（Tokenization）處理後的格式不變，但如果是經過加密（Encryption）處理後的格式，會有所改變。

行動支付運用Tokenization保護信用卡卡號資料的方式



Tokenization
對研究資料的保護方式

傳統對於敏感性資料保護方法，首先會想到 Encryption ，但 Encryption 的結果通常不如預期，通常密文長度會改變，其次是密文為一組不易識別的亂碼，無法再執行分析運用。若採用 Tokenization ，記號化內容可保有原資料特性，如：身分證字號透過 Tokenization ，轉為另一組符合身分證編碼原則之字串，仍可作分析運用。

對從事信用卡使用記錄分析之企業、以身分證字號分析就醫用藥記錄之研究單位，或者是分析消費者行為的組織而言， Tokenization 不失為保護敏感性資料，又可放心從事研究的利器。Tokenization 處理後的資料，除可保有原有資料特性外，因外型與原始資料外型相似，竊取者無法分辨真偽，也就無從破解，能對駭客產生欺敵效果！

Tokenization 技術
為行動支付簡化與安全的關鍵

由於網路購物及行動支付的風行，首先想到的應變作法就是實體信用卡虛擬化與行動化，但單純由信用卡的思維轉換為行動化遭遇到許多整合的問題，如：信用卡整合至NFC手機時，會面臨到多張信用卡與 SIM 卡或 SD 卡整合的問題，交易時，又會面臨到銀行與多家電信公司間下載卡片資訊問題，同時得注意持卡資訊在網路上流通的資安風險。

除了 NFC 手機的近端交易具有卡片資訊外流問題外，大部分電子商務的遠端網路交易的思維仍是以卡片為中心，即使採用軟體模擬負責保護信用卡資訊的 SE （Secure Element）作法，仍無法避免本質上傳遞卡片資訊，存在複製信用卡資訊與盜用的危險。蘋果的 Apple Pay 及 Android 均有志一同地思考根本解決之道，同時指向信用卡號 Tokenization 的技

術，簡單的說，網路上傳送的不再是信用卡號，而是一組隨機對應的字組。而國際組織 EMVCo 也於2014年，對外公開發表正式的 Tokenization Specification 標準，包括蘋果及中國銀聯均採用及推動，Apple Pay 更成為此標準的第一個行動支付系統。

行動支付 Tokenization 技術是以特別的 Token（記號化資料），來替代敏感性資料，如：信用卡號，執行 Tokenization 成為 Token 後，存放於行動裝置上，避免他人直接取得信用卡號等機敏性資料。

實際的信用卡號碼只在最初的請求中使用，在批准或拒絕交易中，返回給請求者的是符號，而不是卡號，儲存在銷售終端（POS）系統中的是 Token ，也不是卡號。
交易時，行動裝置將該 Token 傳至後臺主機，後臺主機可利用此 Token ，找出原本存放於 Token Vault （Tokenization資料庫）的原始卡號，發送一組授權碼交商家，繼續進行後續交易。

行動支付的 Tokenization 技術，主要防止行動裝置本身及傳送過程敏感資料遭到竊取，由於卡號 Tokenization ，使得持卡人的真實資料得以退居幕後，駭客更難獲取。

整體而言， Tokenization 技術支付方式，非常適用於不需出示實物卡的環境，如：行動支付、線上支付等。此外，旅館、健身俱樂部等經常需要儲存臨時交易數據的商家，也非常適合使用此技術。

雲端服務的去識別化防護作法

雲端服務的去識別化與應用系統作法大致相同，應用系統的去識別化作法主導權多掌握在企業手中；而採用雲端服務的企業，因服務資源掌握在雲端資源供應商（微軟與Amazon等）手中，企業可運用雲端資源供應商的去識別化方案，或自建去識別化系統整合雲端資料也是一種彈性作法。在國外， Amazon 的 AWS 雲端服務已與 SafeNet 的 Tokenization Manager 整合，提供雲端資料去識別化服務。雲端資源供應商可持續提供原有雲端服務，企業端可額外執行這些雲端資料去識別化，金鑰及 Token 符號則於企業端保管，確保企業掌握絕對安全主導權。

在產業應用領域上，去識別化作法有些許不同，如：不希望敏感性資料於網路上流通的支付產業等，以 Token 在網路上交換為不錯的選擇；研究或統計分析單位多以 Tokenization 作法為主，於研究分析時，維持 Token 資料擬真性；資訊產業在製作測試性的資料時，為保有資料特性， Tokenization 也較能符合需求，資料以 Token 方式呈現，不以真實資料示人；另提供雲端服務的電商產業為保護客戶資料隱密性，同時保留部分資料可識別性，則多採用 Masking 作法，此一作法，不變動原始資料，僅對外呈現時，以部分樣貌呈現。兩者各有不同運用與安全等級。

參考資料

1. 許世杰，行動支付全面解析 Apple Pay 創造新時代的真正意義，2014, http://punnode.com/archives/23918
2. 洪免，理解行動支付的應用及機制：VISA 圖解說明何謂 TSM、HCE、Visa Token, Nov./18/2014, http://www.techbang.com/posts/20870
3. 翁世吉，行動支付創新之商業營運模式發展趨勢，財金資訊季刊，No.81, Jan./2015, pp.25-34
4. Gemalto SafeNet, Gemalto SafeNet Tokenization.pptx, Jun./2015