付款詞彙表和資訊安全術語

小型商家的資料安全要項
支付卡產業小型商家任務推動小組的成果

2.0 版 | 2018 年 8 月

PCI Security Standards Council®

介紹

這份*付款詞彙表和資訊安全術語*是*安全付款指南*的補充、「小型商家的資料安全要項」內容的一部分。此文件的目的在於使用易於理解的語言解釋相關的支付卡產業 (PCI) 和資訊安全術語。

標有星號 (*) 的術語，其定義是基於或衍生自支付卡產業資料安全標準 **(PCI) 資料安全標準 (DSS) *和支付應用程式資料安全標準 (PA-DSS) 中的定義*：***術語詞彙表、縮寫及縮略字***。**該詞彙表的最新版本被視為是權威資訊來源，必須以此做為目前 PCI DSS 和 PA-DSS 定義的最新完整參考資料。

請參閱以下連結中的小型商家的資料安全要項：

資源	網址
安全付款指南	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
常見付款系統	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
該以哪些問題詢問您的廠商	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf
評估工具	http://www.pcisecuritystandards.org/merchants/ds.org/merchants/ **此工具僅供用於商家資訊。商家可選擇使用此工具作為深入了解其收款方式相關安全實務的第一步，以提供商家初步回覆，並查看其結果**

詞彙表

術語	定義
收單行 *	請參閱商家銀行和支付處理方。
防毒軟體 *	用於偵測、刪除並防禦惡意軟體（也稱為「惡意程式碼」）的軟體程式，惡意軟體包括病毒、蠕蟲，特洛伊程式或特洛伊木馬、間諜軟體、廣告軟體和 Rootkit。也稱為「反惡意程式碼」軟體。
應用程式 *	在 PC、智慧型手機、平板電腦、內部伺服器或網頁伺服器上運作的軟體程式或一套程式。
核准的掃描廠商 (ASV)	經 PCI安全標準委員會核准的公司可以進行外部漏洞掃描服務，以識別系統設定中的常見漏洞。
驗證 *	驗證試圖存取電腦的人員、裝置或程序的身分的措施。身分為了確認身分/使用者是否有效， 會提供以下一或多種措施： • 密碼或複雜密碼（使用者知道的內容） • 使用者（使用者擁有的東西）特有的標記、智慧卡或數位憑證 • 生物特徵識別碼，例如指紋（使用者的特徵或曾經做過的事情）
授權 *	授權是指在支付卡交易中，收單行與簽發者/處理方確認交易後，商家所收到的交易核准。
銀行識別碼 (BIN)	支付卡號的前六位（或更多）數字，用來辨識向持卡人發行支付卡的金融機構。
業務須知	這個原則指的是僅在使用者的業務所需（工作職責所必要）下對其授予系統或資料的存取權。
卡片資料 / 顧客卡片資料	卡片資料至少會包含主帳號 (PAN)，也可能包含持卡人姓名和到期日。PAN 位於卡片的正面，並已編碼到卡片的磁條和/或內嵌晶片中。亦稱為持卡人資料。另請參閱敏感驗證資料以了解其他資料元素，這些資料元素可能是支付交易的一部 分，但不得在交易授權後儲存。
晶片	也稱為「EMV 晶片」。支付卡上用來根據 EMV 交易國際規範處理交易的微處理器（或「晶片」）。
刷卡加密	消費者在購買商品或服務時，在啟用 EMV 晶片的支付終端機中輸入 PIN 碼的驗證過程。

詞彙表

術語	定義
刷卡簽名	消費者在購買商品或服務時，在啟用 EMV 晶片的支付終端機使用其簽名的驗證過程。
憑證	用來識別和驗證使用者以存取系統的資訊。例如，憑證通常是使用者名稱和密碼。憑證可能包括指紋、視網膜掃描或攜帶式「標記產生器」所產生的單次使用號碼。如果存取過程需要多個憑證，表示其安全性較高。
密碼編譯	密碼編譯是透過人或電腦難以理解的資料來保護資料的方法。密碼編譯只有在預期的收件者可以使用僅寄件者和收件者知道的方法將資料重組為可讀形式時才有幫助。另請參閱加密。
網路攻擊	任何侵入電腦或系統的攻擊行為。網路攻擊包括在電腦上安裝間諜軟體、侵入支付系統竊取卡片資料，或試圖破壞重要基礎設施（例如電力網）。
資料外洩	資料外洩是指未經授權的一方可能查看、竊取或使用敏感資料的事件。資料外洩可能涉及卡片資料、個人健康資訊 (PHI)、個人身分資訊 (PII)、商業秘密或智慧財產權等。
預設密碼	新軟體或硬體隨附的簡單密碼。預設密碼（例如「admin」或「password」或「123456」）很容易被猜到，且通常可以透過線上搜尋取得。預設密碼的目的僅是在預留位置，而無法提供真正的安全性，在安裝新軟體或硬體後必須將其變更為強度更高的密碼。
資料安全要項 (DSE)	小型商家的資料安全要項是一套教育資源和評估工具，可協助商家簡化其安全性並降低風險。DSE 是 PCI DSS 自我評估問卷 (SAQ) 的替代方式，適用於支付品牌及收單行（商家銀行）指定合格的商家。
電子收銀機 (ECR)	可以結帳和計算交易，並能夠列印收據，但無法接受客戶使用卡片支付。也稱為「收銀台」(till)。
加密	使用密碼編譯以數學方式將資訊轉換為只有特定數位金鑰的持有者才能使用的格式。加密可降低資訊對於犯罪分子的價值，進而保護資訊。另請參閱密碼編譯。
防火牆 *	保護網路資源以避免遭受未授權的硬體和/或軟體存取。防火牆根據一組規則和其他條件以允許或拒絕具有不同安全層級的電腦或網路間的通訊。

詞彙表

術語	定義
鑑識調查員	PCI鑑識調查員（PFI）是PCI委員會核准的公司，可協助確認卡片資料外洩是在何時以及如何發生。他們採用經實證的調查方法和工具進行金融業相關的調查。他們亦與執法部門合作，以支援利害關係人進行刑事調查。
駭客	試圖繞過電腦系統的安全措施以取得控制和存取權的個人或組織。其動機通常是為了竊取卡片資料。
託管供應商 *	為商家和其他服務供應商提供各種服務，他們為客戶「託管」資料或提供伺服器供客戶的資料常駐。典型的服務包括與個商家共享伺服器空間，為單一商家提供專用伺服器或網頁應用程式（例如提供「購物車」選項的網站）。
整合式支付終端機	結合支付終端機與電子收銀機，可以收款、結帳、計算交易和列印收據。
整合商/經銷商	整合商/經銷商是與商家合作協助建立其支付系統的公司。這可能包括安裝、設定和支援。這些公司可能也提供支付裝置或應用程式的銷售服務。另請參閱*認可整合經銷商 (QIR)*。
記錄 *	在電腦系統或網路中發生某些預先定義（通常與安全性相關）事件時自動建立的檔案。記錄檔資料包括日期/時間戳記事件描述以及該事件的唯一資訊。這些檔案在解決技術問題或調查資料外洩露時會很有幫助。也稱為「稽核記錄」或「稽 核線索」。
惡意程式碼 *	設計用來滲透到電腦系統中的惡意軟體，目的在竊取資料或破壞應用程式或作業系統。作業系統這種軟體通常會在許多商業核准的活動（例如透過電子郵件或瀏覽網站）期間進入網路。惡意程式碼的範例包括病毒、蠕蟲、特洛伊程式（或特 洛伊木馬）、間諜軟體、廣告軟體和Rootkit。
商家銀行 *	商家銀行是替商家處理信用卡和/或轉帳卡支付的銀行或金融機構。此類實體也稱為收單行、收單銀行、卡片處理方或支付處理方。
行動裝置	小型、可攜且可無線連接到電腦網路的裝置，例如智慧型手機和平板電腦。
行動支付收款	使用移動裝置接受和處理支付交易。移動裝置通常會與市售的讀卡機配件配對。

詞彙表

術語	定義
多重要素驗證 *	在進行使用者身分驗證時驗證兩個或更多因素的方法。這些因素包括使用者擁有的東西（例如智慧卡或硬體鎖）、使用者知道的東西（例如密碼、複雜密碼或 PIN 碼），或使用者的身分或行為（例如指紋、其他形式的生物特徵等）。
網路 *	透過實體或無線方式連接的兩台或更多電腦。
作業系統 *	電腦系統上的軟體，用來管理和協調整體電腦活動。範例包括 Microsoft Windows、Apple OSX、iOS、Android、Linux 和 UNIX。
P2PE	PCI安全標準委員會的「點對點加密」(Point-to-Point-Encryption) 標準的縮寫。詳情請參閱 www.pcisecuritystandards.org
PA-DSS *	PCI 安全標準委員會的「支付應用程式資料安全標準」(Payment Application Data Security Standard) 的縮寫。詳情請參閱 www.pcisecuritystandards.org
密碼 *	用於驗證使用者身分的單詞、片語或字元字串。將密碼與使用者名稱合併使用，可證明使用者的身分以存取電腦資源。
修補程式 *	更新現有軟體以新增功能或修正缺陷（或「錯誤」）。
支付應用程式 *	支付應用程式與 PA-DSS 相關，是在授權或結算支付交易時用來儲存、處理或傳輸持卡人資料的軟體應用程式。
支付應用程式廠商	此供應商販售在付款交易期間儲存、處理和/或傳輸卡片資料的應用程式。
支付中介軟體	此術語是用來統稱將兩個或多個（可能不相關）支付應用程式連接在一起的軟體。例如，此類軟體可以在支付終端機的應用程式和其他傳送卡片資料至處理方的商家系統之間傳遞卡片資料。
支付處理方*	此實體受商家委託，代表他們處理支付卡交易。雖然支付處理方通常提供收單服務，但除非支付卡品牌特別定義，否則收單處理方不會被視為收單機構（商家銀行）。也稱為「支付網關」或「支付服務供應商」(PSP)。另請參閱商家銀行。
支付系統	包含在商家零售場所（包括商店和電子商務店面）接受卡片支付的整個過程，可能包括支付終端機、電子收銀機，其他設備等 或連接到支付終端機的系統（例如，用來連線的 Wi-Fi 或用來管理庫存的電腦）、具有電子商務元件（例如支付頁面）的伺服器以及與商家銀行的連線。

詞彙表

術語	定義
支付系統供應商	向商家出售、授權或發佈完整支付解決方案的供應商。該解決方案包括處理方店內支付所需的硬體和軟體，並提供連接支付處理方的方法。
支付終端機	透過刷卡、插卡、點擊來接受客戶卡片支付的硬體設備。也稱為「銷售點 (POS)」，「刷卡機」或「PDQ 終端機」。
PCI *	支付卡產業 (Payment Card Industry) 的縮寫。
PCI DSS *	PCI 委員會的「支付卡產業安全標準」(Payment Card Industry Data Security Standard) 的縮寫。詳情請參閱 www.pcisecuritystandards.org
符合 PCI DSS	常態營業的方式能持續符合 PCI DSS 目前所有適用的要求。合規性的評估和驗證是在單一時間點進行；但若要確保強健的安全性，商家必須持續遵循要求。商家銀行和/或支付品牌可能對 PCI DSS 合規性的年度正式驗證另有規定。
經 PCI DSS 驗證	提供在單一時間點符合所有適用 PCI DSS 要求的證明。根據特定商家銀行和/或支付品牌的要求，可以透過適用的 PCI DSS 自我評估問卷或透過現場評估取得的合規性報告來完成驗證。
PCI 驗證的支付應用程式	經 PCI 支付應用程式資料安全標準 (PA-DSS) 驗證並在 PCI 委員會網站上列出的軟體應用程式。
PCI 核准的支付終端機	已根據 PCI PIN 碼交易安全 (PTS) 標準所核准，並在 PCI 委員會網站上列出的付款終端機。
PCI 清單所列的點對點加密解決方案	已根據 PCI 清單所列的點對點加密 (P2PE) 標準所驗證，並在 PCI 委員會網站上列出的加密解決方案。
PED *	「PIN 碼輸入設備」(PIN entry device) 縮寫。客戶用來輸入 PIN 碼的鍵盤。也稱為「密碼鍵盤」(PIN pad)。
PIN *	「個人識別碼」(personal identification number) 的縮寫。只有使用者和系統知曉的獨有編號，用來向系統驗證使用者的身分。典型的 PIN 碼用於自動提款機以進行預借現金交易，或用於代替 EMV 晶片卡持卡人的簽名。PIN 碼可協助確認持卡人是否被授權使用該卡片，並在卡片遭竊盜後防止未經授權的使用。
主要帳戶號碼 (PAN) *	信用卡和轉帳卡的獨有編號，用於標識持卡人帳戶。

詞彙表

術語	定義
濫用特權	濫用電腦系統的存取權限。例如，系統管理員出於惡意目的存取卡片資料，或某人出於惡意目的竊取和使用管理員較高權 限的存取權 。
PTS *	PCI 委員會的「PIN 交易安全」(PIN Transaction Security standard) 的縮寫。PTS 是針對 PIN 碼接受獨立互動點 (POI) 終端機的一套模組化評估要求。詳情請參閱 www.pcisecuritystandards.org
QIR *	「認可整合商或經銷商」(Qualified Integrator or Reseller) 的縮寫。QIR 是經過 PCI 安全標準委員會專門訓練的整合 商和經銷商，可以在安裝商家支付系統時解決關鍵的安全控制問題。詳情請參閱 www.pcisecuritystandards.org
合格安全評估機構 (QSA)*	經 PCI 安全標準委員會核准，以驗證實體是否遵守 PCI DSS 要求的公司。
週期性支付	商家定時重複向其顧客收費的一種計費方式，例如月費會員資格或訂閱。安全的做法是讓收單行/處理方標記化卡片資 料，以確保對卡片內容的保護並減輕商家的責任。
遠端存取 *	從網路之外的位置存取電腦網路。遠端存取連線可能會來自公司本身內部網路，也可以來自遠端位置。虛擬私人網路 (VPN) 是遠端存取技術的其中一個範例。遠端存取可能來自內部（例如，IT 支援）或外部（例如，服務供應商、第三方代理 機構、整合商/經銷商）。
經銷商 / 整合商 *	出售和/或整合支付應用程式但不開發支付應用程式的實體。
路由器 *	連接兩個或多個內部或外部電腦網路以透過網路「路由」或引導資料，並確保資料在這些網路間正確流動的硬體或軟體。路由器也可以透過僅允許核准的流量並拒絕未核准的流量來建立更高的安全性。
安全讀卡機 (SCR)	經 PTS 核准的設備，可連接到手機或平板電腦以安全地接收支付卡。經 PCI PTS 核准的 SCR 透過 SRED 保護並加 密卡片資料。另請參閱 *SRED*。
安全碼 *	支付卡正面或背面簽名欄中印刷的三位數或四位數的值。此代碼僅與單一卡片相關聯，並用來進行額外檢查，通常是在無卡交易中確保該卡片由合法持卡人擁有。也稱為卡片安全碼。

詞彙表

術語	定義
自我評估問卷 (SAQ) *	一份由組織本身完成的調查問卷，內容涵蓋一套 PCI DSS 要求，用以確認該組織符合這些要求。
敏感驗證資料 *	儲存在卡片磁條或晶片上，用於驗證持卡人身分和/或授權支付卡交易的安全相關資訊。
服務供應商 *	為商家提供各種服務的企業實體。通常，這些實體代表另一個實體（例如商家）儲存、處理或傳輸卡片資料，或者是提供 託管防火牆、入侵偵測、託管以及其他 IT 相關服務的託管服務供應商。也稱為「廠商」(vendor)。
側錄	直接從消費者的支付卡或從商家位置的支付基礎設施竊取卡片資料，例如使用未授權的手持式讀卡器或修改商家的支付 終端機。其目的是進行詐欺，這是很嚴重的威脅，且任何商家的環境都可能受到攻擊。
側錄裝置	通常是用來連接到讀卡裝置的一種實體裝置，目的在非法擷取和/或儲存來自支付卡的資訊。也稱為「卡片側錄」(card skimmer)。
小型商家	小型商家通常是獨立擁有、只在單一或數個地點經營的企業，其 IT 預算有限或沒有預算，且通常沒有 IT 人員。 小型商家是否需要驗證 PCI 合規性是由支付品牌或收單行（商家銀行）來決定。
SRED	「安全讀取和資料交換」(Secure Reading and Exchange of Data) 的縮寫。這是一套 PCI PTS 要求，目的在保護和加密支付終端機中的卡片資料。PCI 委員會所列的點對點加密 (P2PE) 解決方案必須使用經 PTS 核准並列出，且啟用 SRED 及主動執行卡片資料加密的支付終端機。
獨立終端機	不需與商家環境中的任何其他設備連線，且不執行其他功能的支付終端機。 唯一的操作要求是透過網路連線或電話線與處理方連線。 如果終端機需要連接到電腦化的電子收銀機或者是多功能的裝置（例如行動裝置），便不屬於獨立終端機。
強式驗證	用於驗證使用者或裝置的身分，以確保所保護系統的安全性。術語「強式驗證」通常是指使用多重要素驗證 (MFA)。
收銀台	請參閱電子收銀機。
標記化	用稱為標記的替代值替換主要帳戶號碼 (PAN) 的過程。標記可以在卡片不在手邊時代替原始的 PAN 來執行功能，例如取消交易、退款或週期性支付。標記就算遭竊也無法使用，對犯罪分子沒有任何價值，因此能提供更高的安全性。

詞彙表

術語	定義
未加密的資料	不需要先解密就可以讀取的資料。也稱為「純文字」(plaintext/clear-text) 資料。
廠商	為商家提供業務過程所需的產品或服務的企業實體。廠商在提供服務的地方會被視為服務供應商，且可能需要存取商家環境中可能影響卡片資料安全性的實體位置或電腦系統。另請參閱服務供應商。
虛擬支付終端機 *	透過網頁瀏覽器存取收單機構、處理方或第三方服務供應商網站以授權支付卡交易。 虛擬終端機與實體終端機的差別在於虛擬終端機不會直接讀取支付卡資料。 商家透過安全連接的網頁瀏覽器手動輸入支付卡資料。 由於支付卡交易是經由手動輸入，因此在交易量較小的商家環境中通常會使用虛擬支付終端機代替實體終端機。
虛擬私人網路 (VPN) *	可建立安全的私人通道，並透過網路交換資料並進行通話的軟體。
病毒	將自己的副本複製到「受感染」電腦上的其他軟體或資料檔案中的惡意程式碼。病毒在複製後可能會執行惡意裝載，例如刪除電腦上所有的資料。病毒可能會先處於休眠狀態並在稍後才執行其裝載，也可能永遠不會觸發惡意行為。用電子郵件附件或網路訊息的形式將自己重新傳送以自行複製的病毒稱為「蠕蟲」。
弱點 *	系統的缺陷或弱點，如果遭到濫用，可能會有意或無意地導致系統受損。
漏洞掃描	用於偵測和分類電腦或網路上潛在弱點（漏洞）的軟體工具 根據 PCI DSS 11.2.2 要求的季度外部漏洞掃描必須由經核准的人員執行掃描供應商。 其他漏洞掃描（如內部掃描和網路變更後執行的掃描）可由組織 II 部門中合格的人員或安全服務供應商（例如核准的掃描供應商）進行。另請參閱核准的掃描廠商 (ASV)。
Wi-Fi *	無需連接實體線路即可連接電腦的無線網路。
無線支付終端機	使用各種無線技術連線到網際網路的支付終端機。