商店安全性

系統升級指南

點選此處並查看遵守 SHA-256 業界標準的資訊。

協助完成經得起未來考驗的整合工作

全球安全威脅瞬息萬變，因此捍衛商店的安全一直是我們首要的任務。為防範現今及未來的威脅，我們建議你進行下列的整合升級：

1. 停止使用 VeriSign G2 根憑證。
2. 更新整合以支援採用 SHA-256 演算法的憑證。

為什麼要進行變更？

公共憑證授權（Certificate Authority，簡稱 CA）業界不斷提升 SSL 憑證的安全性。為因應 2016 年全面改用 SHA-256 簽署演算法的要求，我們將不再支援 VeriSign G2 根憑證。該憑證以往用於連接 PayPal 應用程式介面 (API) 和交易狀態更新 (IPN) 端點。

需在何時採取行動？

請立刻採取行動，以因應這些變動。

如需詳細的時間表，例如：正式環境和 Sandbox API 端點的升級日期，請參閱 2015-2016 SSL 憑證變更微型網站。

NOTE: 這些變更是為了因應整個業界面臨的安全威脅，並非單獨針對 PayPal 實施。導入這些變更後，PayPal 整合作業的隱私與穩定度將可提升。由於這些變更的詳細資料會因不同系統而有所差異，建議你在執行變更時尋求合格的系統管理員協助。

1. 停止使用 VeriSign G2 根憑證

問題：以往 VeriSign 核發的 SSL 憑證均包含由 1024 位元 G2 根憑證簽署的信任鏈。而近年來，美國政府與公共憑證授權業界已轉向更安全的 2048 位元憑證，因此目前 VeriSign 所核發的 SSL 憑證均包含由 2048 位元 G5 根憑證（2006 年核發）簽署的信任鏈。

我們的回應：為符合業界標準，凡是需要由 G2 根憑證簽署憑證 / 信任鏈的 API/IPN 端點安全連線，我們將不再受理。只有需要由 G5 根憑證簽署憑證 / 信任鏈的安全連線要求，才可以成功完成安全連線。

你必須：

若系統目前要求使用包含 G2 識別碼的 VeriSign 根憑證，你必須將依賴這類根憑證的 SSL 連線停用。業界正積極在今年逐步淘汰 1024 位元根憑證。

- 凡是依賴由 G2 根憑證簽署憑證鏈的安全連線將無法受到支援：

組織單位	Class 3 Public Primary Certification Authority - **G2**
序號	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
憑證 SHA1 指紋	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- 凡是依賴由 G5 根憑證簽署憑證鏈的安全連線將會受到支援：

一般名稱	VeriSign Class 3 Public Primary Certification Authority - **G5**
序號	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
憑證 SHA1 指紋	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

請依照這些指示操作，以確保你使用受支援的 VeriSign G5 根憑證安全連線：

1. **檢查你的憑證存放區。**請你的網站代管者或系統管理員提供協助，確認目前由驗證邏輯碼使用的根憑證存放區是否有 VeriSign G5 根憑證。如果有，則無需採取行動。
   - 請查看下列連結，檢查你的金鑰存放區是否有使用 Java、Linux 或 Windows 的 G5 根憑證。
2. **檢查你的錯誤記錄。**若你尚未下載 VeriSign G5 根憑證來取代 G2 根憑證，可能會看到下列的錯誤訊息：
   - SSL 信號交換錯誤：“No trusted certificate found”（找不到受信任的憑證）
   - 結果碼 -31：“The certificate chain did not validate, no local certificate found”（憑證鍊未認證；找不到本機憑證）
   - 結果碼 -8：“SSL connection failed”（SSL 連接失敗）
   - - 1 錯誤

   若要解決這些問題，你可以執行下列其中一項操作：

   - 將軟體更新為支援 SHA-256 的最新版本，或者
   - 若將金鑰存放區作為驗證或授權憑證之用，請將 VeriSign G5 根憑證安裝至金鑰存放區。
3. **取得 VeriSign G5 根憑證。**若你的憑證儲存區或 Java 用戶端未包含 VeriSign G5 根憑證，請要求系統管理員從 VeriSign 下載根憑證，並將根憑證儲存在憑證儲存區和任何其他 SSL 連線授權套件中。
   - 下載 Symantec 的 VeriSign G5 根憑證
   - 若你的伺服器需要，請下載特定伺服器的 SSL 憑證

2. 更新至 SHA-256 簽署演算法

問題：加密演算法 SHA-1 已有 22 年歷史，受到日益強大的運算能力所威脅。SHA-256 採用的演算法包含 256 位元雜湊值，因此較為安全。

我們的回應：我們將於 2016 年中期升級所有正式環境和 Sandbox 端點的 SSL 憑證，SHA-1 演算法將會升級為較穩固的 SHA-256 演算法。

你必須：

依照指示操作，將運用 SHA-1 簽署演算法的 SSL 憑證改為較強大的 SHA-256 簽署演算法：

1. **檢查你的系統環境。**確認你的環境支援 SHA-256 憑證。
   - 請參考「DigiCert 的 SHA-2 相容性指南」和「Symantec 支援的瀏覽器與伺服器清單」等線上資源，以了解有支援的硬體和軟體清單。
   - 若部分環境不支援 SHA-256，你需要在導入新憑證前，先替換或升級這些元件。
   - Windows 2000 Server 和 Windows XP 的某些版本可能與 SHA-2 不相容。這個有關 SHA2 和 Windows 的 Windows PKI 部落格可以提供修補程式方面的協助，同時給予有關升級系統環境的建議。
2. **檢查你的憑證。**若你的系統環境支援 SHA-256，請確保你的金鑰存放區具有 VeriSign G5 根憑證。

有任何的問題嗎？

如需其他資料或常見問題，請參閱
2015-2016 SSL 憑證變更微型網站。

感謝你！

感謝你及時注意此問題，並理解我們的做法。我們知道這些步驟可能會導致相容性問題，但是短時間內的不便，遠不及我們保護客戶帳戶及財務資料安全之承諾來得重要。