商家安全資訊

系統升級指南

按一下此處，查看遵守 SHA-256 業界標準的資訊。

升級整合方式，為未來做好準備

全球性的安全威脅日新月異，而我們一直致力以保護商家安全為首要任務。為防範當前和未來的威脅，我們建議你採取以下行動，以升級整合方式：

1. 停止使用 VeriSign G2 根源證書。
2. 更新你的整合方式，以支援使用 SHA-256 運算法的證書。

為何要變更？

公共數碼證書認證機構 (CA) 行業持續提升 SSL 證書的安全性。為預備在 2016 年使用 SHA-256 簽章運算法的要求，我們將不再支援 VeriSign G2 根源證書。此證書過往用於連接到 PayPal API 和即時付款通知 (IPN) 端點。

我需要何時採取行動？

請立刻採取行動，以因應這些變動。

如要了解詳細的時間安排，包括實際使用端點和 Sandbox API 端點的升級日期，請參閱 2015 年至 2016 年 SSL 證書變更微網站。

NOTE: 這些變更是為了解決行業整體的保安問題而實施，並非 PayPal 單方面要求。實施後，可提升 PayPal 整合方式的私隱度和可靠度。由於這些變更的細節因系統而異，我們建議你在合資格系統管理員的協助下執行。

1. 停止使用 VeriSign G2 根源證書

問題說明：過去，VeriSign 發行的 SSL 證書使用 1024 位元的 G2 根源證書簽章作為信任鏈。近年來，美國政府及公共數碼證書認證機構 (CA) 行業已轉用安全性更高的 2048 位元證書，因此，VeriSign 現時發行的 SSL 證書使用在 2006 年發佈的 2048 位元 G5 根源證書簽章作為信任鏈。

我們的回應：按照行業標準，我們將不再繼續接受預期我們使用 G2 根源證書簽章作為的證書 / 信任鏈的 API/IPN 端點安全連線。只有預期我們使用 G5 根源證書簽章作為的證書 / 信任鏈的安全連線要求才可以成功地進行安全連線。

你必須採取的行動…

如果你的系統目前強制要求使用 VeriSign 根源證書，必須停止使用以 G2 作為識別碼的證書進行 SSL 連線。業界正主動尋求在本年內逐步停用 1024 位元根源證書。

- 倚賴我們以 G2 根源證書簽章作為證書鏈的安全連線將不獲支援：

組織單位	第 3 類公共一級認證機構 — **G2**
序號	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
證書 SHA1 指紋	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- 倚賴我們以 G5 根源證書簽章作為證書鏈的安全連線將獲得支援：

通用名稱	VeriSign 第 3 類公共一級認證機構 — **G5**
序號	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
證書 SHA1 指紋	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

要確保你使用獲支援的 VeriSign G5 根源證書進行安全連線，請遵照以下指引操作：

1. **檢查你的證書儲存庫。**要求你的網站代管機構或系統管理員驗證你在程式碼中用作驗證邏輯的 VeriSign G5 根源證書是否包含在根源儲存庫之中。如果包含在內，則無需採取任何行動。
   - 進入以下連結，以檢查你使用 Java、Linux 或 Windows 的 G5 根源證書是否包含在你的密鑰儲存庫之中。
2. **檢查你的系統錯誤記錄。**如果未有下載 VeriSign G5 根源證書來取代 G2 根源證書，你就可能會看到以下錯誤訊息：
   - SSL 交握錯誤：「No trusted certificate found」
   - 結果代碼 -31：「The certificate chain did not validate, no local certificate found」
   - 結果代碼 -8：「SSL connection failed」
   - -1 error

   要解決這些問題，你可以採取以下其中一項行動：
   - 更新你的軟件為支援 SHA-256 的最新版本，或
   - 如果你有使用密鑰儲存庫作證書驗證 / 認證之用，安裝 VeriSign G5 根源證書到你的密鑰儲存庫之中。
3. **取得 VeriSign G5 根源證書。**如果你的密鑰儲存庫或 Java 用戶端程式不包含 VeriSign G5 根源證書，就需要要求你的系統管理員從 VeriSign 下載並儲存到證書儲存庫以及其他 SSL 連線認證套件之中。
   - 下載 Symantec 的 VeriSign G5 根源證書
   - 下載特定的伺服器 SSL 證書（如要伺服器有此要求）

2. 更新為 SHA-256 簽章運算法

問題說明：SHA-1 是 22 年前面世的加密運算法，由於電腦的運算功能日益強大，此運算法的安全性備受威脅。SHA-256 使用的運算法較 256 位元雜湊值更安全。

我們的回應：我們將會在 2016 年年中將所有實際使用端點和 Sandbox 端點的 SSL 證書從 SHA-1 升級到更安全和更嚴密的 SHA-256。

你必須採取的行動…

請按照這些指示，將使用 SHA-1 簽章運算法的 SSL 證書逐步轉為更安全的 SHA-256 簽章運算法：

1. **檢查你的系統環境。**確保你的系統環境支援 SHA-256 證書。
   - 參考網上資源，例如 DigiCert 的 SHA-2 兼容性指南和 Symantec 的支援瀏覽器和伺服器清單，所有支援的軟硬件均已詳細列出。
   - 如果你的部分系統環境不支援 SHA-256，就需要更換或升級相關部分，然後才可以採用新證書。
   - Windows 2000 伺服器和部分版本的 Windows XP 可能不兼容 SHA-2。這個 Windows PKI 網誌有關 SHA2 和 Windows 的文章有助你找出升級系統環境所需的修正程式和建議方案。
2. **檢查你的證書。**如果你的系統環境支援 SHA-256，請確保你的密鑰儲存庫之中包含 VeriSign G5 根源證書。

有疑問嗎？

如需查看其他詳情和常見問題，請瀏覽我們的 2015 年至 2016 年 SSL 證書變更微網站。

多謝你的支持！

感謝你及時處理此問題，並理解我們的做法。我們明白這些步驟可能會導致兼容性問題，雖然此舉會造成短暫不便，但它有助確保客戶的帳戶及財務資料安全，讓你我一同實踐對客戶的安全承諾，長遠來說能夠帶來極大裨益。