



* 白皮書

安全與信任：
透過網際網路進行交易的基礎



目錄

+ 簡介	3
+ 加密技術與 SSL 憑證	4
加密等級與 SGC	5
驗證與信任等級	5
+ 延伸驗證 (EV) 是信任的新標準	7
+ VeriSign SSL 憑證, 最堅實的安全與信任	9
+ 結論	10



安全與信任： 透過網際網路進行交易的基礎

+ 簡介

對於要求客戶透過網路提供敏感資料的任何一家公司來說，取得線上客戶的信任是成功致勝的關鍵。在電子商務中，消費者非常擔心身分遭人盜用，因此對於提供個人資訊給不信任的來源自然有所疑慮，尤其是為了支付交易款項而提供的信用卡號碼。其他類型的線上交易需要的資訊雖然不同，但卻一樣敏感。一般人都不太願意提供社會安全號碼、密碼、醫療和其他機密的個人資訊，有些人甚至連姓名、地址和電話號碼也不願意提供。因為他們害怕這些資訊可能會在傳送的過程中遭到攔截，或者目的地本身是由意圖不軌的詐欺者所操縱。

許多謹慎的消費者最後都會選擇放棄交易。事實上，根據 TNS Research 在 2006 年提出的報告顯示，70% 的線上購物者曾經因為安全上的顧慮而放棄購物。其他購物者可能克服了恐懼而進行小額的購買，但是會限制交易的金額大小，因為他們擔心自己可能付了錢卻拿不到任何商品。

消費者的這種恐懼其來有自。在 2007 年的線上收益中，線上詐欺所造成的損失估計約有 36 億美元 — 比 2006 年上升了 16%¹。2008 年 1 月份提報給「防制網路釣魚工作小組」(Anti-Phishing Working Group, APWG) 的特殊網路釣魚報告總數為 29,284 件，比前一個月增加了將近 9%²。

若能消弭客戶的恐懼，線上業務仍然有很大的獲利空間。對於網際網路詐騙的擔憂是銷售業績的一大阻礙。TNS Research 在 2006 年 8 月提出的報告顯示，有 87% 的線上購物者非常擔心信用卡詐騙，而有 83% 則對於分享個人資訊有所疑慮。由於對犯罪的恐懼不只限制了交易的次數也限制了交易的金額，因此透過建立信任所能獲得的潛在商機實際上非常龐大。

此外，消費者也能透過打破這道信任的藩籬而獲益良多。線上購物的便利性和價格具有極大的優勢。在選購特定的商品時，通常消費者不僅會在可信任的網站找到這項商品，也會在收費較低或是提供其他優惠的網站上找到這項商品。如果能夠有一種可以在非知名品牌網站上快速取得信任的方法，對消費者來說不是更為有利嗎？但是對於身分盜用的恐懼（根據 2006 年 8 月的 TNS 研究，85% 的購物者有這樣的恐懼）顯然讓許多消費者無法享受這些好處 — 事實上，根據 Forrester Research 在 2006 年 12 月所做的調查，24% 的購物者完全沒有在線上購物。

幸好現在已經有一項技術可以幫助線上企業保護敏感的客戶資料、證明自己的身分，以及建立消費者的信任；這項技術也可以幫助客戶分辨哪些網站值得信任，哪些網站是意圖不法的詐騙人士所架設的冒牌網站。

¹ Cybersource, 《9th Annual Online Fraud Report》(第 9 期年度線上詐欺報告), 2008 年

² APWG, 《Phishing Activity Trends》(網路釣魚活動的趨勢), 2008 年 1 月

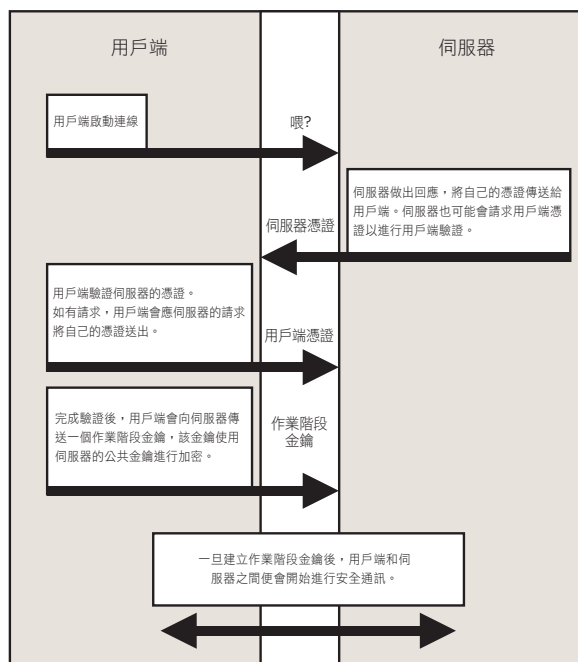
本白皮書將探究這項技術目前的發展狀況，以及 VeriSign Inc. 對於幫助組織保護重要資料並讓客戶產生信任所做的貢獻。文中首先討論加密和 Secure Sockets Layer (SSL)；這種技術解決了最明顯也是線上業務固有的問題 — 傳送的資料非常容易遭到網路犯罪者的攔截。但是加密技術已經不足以應付愈來愈複雜的網際網路竊盜手法。因此，接下來本白皮書將提出近來變得更為重要的驗證和建立信任等問題，並介紹可以解決這些問題的延伸驗證 (EV) SSL 技術。最後，我們將介紹在上述所有安全技術中，能夠提供最強大功能的 VeriSign® 方案。

+ 加密技術與 SSL 憑證

客戶都知道，當他們將任何資訊提交給不安全的網站時，都必須承受極大的風險。因此，為了在市場上生存，電子商務公司必須將 SSL 憑證與他們所採用的加密技術結合在一起。

加密是將資訊進行轉換，使指定收件者以外的所有人都無法理解該項資訊的一種程序。加密是電子商務所需資料完整性和隱私權的基礎。只有在確信自己的敏感資訊安全無虞時，客戶和商業合作夥伴才會透過網路將敏感資訊和交易提交到您的網站。對於注重電子商務的企業來說，這個問題的解決方法就是實施一套以加密技術作為基礎的電子商務信任架構。

Secure Sockets Layer (SSL) 是網路安全的全球標準，也是用來加密及保護利用普及的 HTTP 通訊協定在網路上傳輸之資訊的技術。SSL 可以保護移動中的資料，避免因為以未加密的方式傳送而遭到攔截或竄改。所有的重要作業系統、Web 瀏覽器、網際網路應用程式和伺服器硬體中都已內建 SSL 支援。



SSL 憑證是一種電子檔案，可以用來識別個人和網站的唯一身分，以及啓用加密通訊。SSL 憑證可當作一種數位護照或數位認證。SSL 憑證的「簽署者」是憑證管理中心 (CA)。VeriSign 無疑是全球頂尖的 CA，因為我們為全世界超過 1 百萬台的 Web 伺服器提供安全防護³。

下圖顯示可保障 Web 伺服器和用戶端間通訊安全防護的流程。SSL 憑證的所有交換作業都只需花費數秒鐘，而且客戶不需要採取任何動作。

³ 包括 VeriSign 的子公司、聯盟機構與經銷商。

加密等級與 SGC

加密分成各種不同的強度，實際的強度是依加密演算法所使用的位元數目決定。現行標準是 128 位元，也是公認實質上駭客無法以目前的電腦運算速度破解的一種強度。某些舊版的作業系統和瀏覽器，在特定的組合下（包括許多 Windows 2000 系統），無法支援超過 40 或 56 位元的加密。這些等級現在很容易被破解，也使得這些作業系統和瀏覽器組合的使用者暴露在威脅之下。

某些 VeriSign SSL 憑證提供了一種名為「伺服器閘道型加密」(Server-Gated Cryptography, SGC) 的技術，幫助 99.9% 的網站訪客解決這個問題。(某些舊版瀏覽器無法處理任何 SSL 憑證提供的 128 位元加密。)採用 SGC 的網站將會「升級」到 128 位元加密，以便與通常只能執行 40 或 56 位元加密的系統進行通訊。因此，使用 SGC SSL 憑證的企業可以確保所有的客戶都能採用最高的加密等級。VeriSign 安全網站專業版和使用 EV 的安全網站專業版可支援 SGC 128 位元加密。在用戶端和伺服器都能以 256 位元等級進行加密的所有連線，所有的 VeriSign SSL 憑證都能支援最高 256 位元的加密。

驗證與信任等級

SSL 憑證的主要用途之一是向消費者保證他們正在進行交易的網站確實是自己想要造訪的網站。因此，CA 在核發憑證之前都會進行驗證檢查工作。一般公認的 SSL 驗證可分為三大類別：網域驗證、組織驗證和 EV；這些類別在提供的安全與信任等級中的差異極為重要。即使是同一個等級，某些驗證程序也會隨著不同的 CA 而改變 — 這是您應該選擇知名、權威且值得信任的 CA 的主要原因。其他 CA 受到信任的程度和知名度都不如 VeriSign。

網域驗證

網域驗證型憑證是可用的驗證形式中等級最低的一種。CA 將會進行一套程序，以驗證申請網域驗證型憑證的實體是否擁有申請的網域或有權使用該網域名稱。他們可能也會驗證申請憑證的連絡人的電子郵件地址是否列在 WHOIS 工商名錄中，或者是否符合該 CA 制定的電子郵件別名需求事項。VeriSign 並未提供網域驗證型 SSL 憑證。

組織驗證

組織驗證是 VeriSign 和其他 CA 針對一般 (非 EV) SSL 憑證所採用的驗證程序。CA 一開始會先透過政府發放的企業證書來驗證組織是否確實存在 (通常是藉由搜尋政府和私人資料庫的方式)。如果有需要，他們可能還會要求組織提供公司章程、公司執照和虛擬名稱聲明之類的文件。在核發 SSL 憑證之前，CA 會驗證公司的身分並確認它是法人實體、確認該公司有權使用憑證中所含的網域名稱，並驗證代表公司申請 SSL 憑證的個人有權提出申請。



延伸驗證

EV (將於下一節討論) 擁有 SSL 憑證可提供的最高驗證等級。EV 驗證增加了組織驗證流程的結構和控制功能。一開始它會先要求企業聯絡人提出已簽署的合約確認書, 以便就實體的正統身分進行深入的驗證。如果 CA 無法透過政府機關的資料庫來確認組織詳情, 可能還會要求組織提供公司註冊文件。另外可能也需要法律意見書, 以便確認組織的下列詳細資料:

- 業務營運地點的實體地址
- 電話號碼
- 網域獨佔使用權的實證
- 組織確實存在 (如果少於 3 年) 的其他實證, 以及
- 企業聯絡人員工身分的證明。

這套流程對於合法組織來說只是一點小工作, 但卻是詐騙集團的一大阻礙。

信任標記

為了贏得信賴並拓展線上業務, 您不只需要保護客戶的線上傳輸, 也必須讓客戶知道您已經這樣做。因此, CA 都會為您提供帶有其信任標記的認證標章, 供您張貼在網站的不同頁面。底下顯示的 VeriSign® 全球安全網站認證標章是全球最普及也是最知名的安全認證標章。只要按一下這個認證標章, 就會出現一個畫面, 顯示憑證擁有者的名稱、效期, 以及提供的安全防護等級與 VeriSign 在核發憑證之前所採取的驗證程序等相關資訊。在 TNS Research 報告中指出曾經因為顧慮安全問題而放棄購物車的 70% 線上購物者中, 有高達 90% 的人表示如果當初網站上有 VeriSign Secured 全球安全網站認證標章, 他們就會完成交易。⁴



⁴ TNS Research, 2006 年 8 月

+ 延伸驗證 (EV) 是信任的新標準

SSL 作業階段的指標，例如 URL 中的 “https” 或是金色鎖頭圖示，提供了以充足的加密等級保護敏感資料傳輸的保證；在過去，這樣的保證便足以消弭多數消費者的疑慮。但是現在因為出現了非常不一樣的問題，所以即使是最強的加密也已經不夠了。網際網路竊賊已經變得非常善於偽裝成真正的電子企業。他們會購買 SSL 憑證 — 遺憾的是，他們非常容易就能從背景調查工作不確實的 CA 取得憑證 — 並使用這些憑證誘騙客戶傳送敏感資訊給他們。這就是加密已經不足的原因 — 如果加密傳輸的接收者是冒牌企業，並繼續利用加密傳輸來從事身分盜用或其他不法行為，那麼加密反而沒有任何好處。那麼一般民眾要如何判斷自己不熟悉的網站確實是合法網站呢？而且，就算是看似知名、受信任的線上企業網站，一般人又該如何確定它不是某個狡猾且意圖不軌的詐欺者所架設的冒牌網站呢？有 90% 的使用者無法區分網路釣魚網站和合法網站⁵。

為了獲得客戶的信任，您需要一種簡單但可靠的方法，除了向客戶證明他們的交易非常安全以外，也能夠證明您是合法企業，而且您的身分絕對真實無誤。為了因應這項需求，安全服務供應商和網際網路瀏覽器通力合作，建立了延伸驗證 (EV) 標準，這也是十多年來全球安全電子商務基礎第一次的重大改變。VeriSign 的延伸驗證 SSL 憑證便是採用這套標準。

當客戶瀏覽受 EV SSL 憑證保護的網頁時，只要他們使用的是具有 EV 功能的瀏覽器版本，網址列就會變成綠色。目前和未來版本的 Microsoft Internet Explorer (從 Internet Explorer 7 開始)、Firefox (從 Firefox 3 開始) 和 Opera (從 Opera 9.5 開始) 都擁有這項功能。在現今使用的瀏覽器中，這些瀏覽器和具有 EV 功能的其他瀏覽器所佔的比例已超過 50%⁶。

除了變成綠色之外，瀏覽器也會顯示憑證中列出的組織名稱 (例如您的公司)。執行細節會因為不同的瀏覽器而稍有出入。以 IE7 為例，它會顯示憑證的安全服務供應商名稱 (如 VeriSign) 以及組織的名稱，並切換顯示這兩個名稱，如同下圖所示。

圖 2：綠色網址列和延伸驗證



⁵ Rachna Dhamija, 哈佛大學; J.D. Tygar, 加州大學伯克萊分校; Marti Hearst, 加州大學伯克萊分校

⁶ Net Applications, 《MarketShare Report》(市場佔有率報告), 2008 年 8 月

使用 EV 的 VeriSign 安全網站專業版 SSL 憑證使每一位網站訪客都能夠採用最強的 SSL 加密，並提供最高的信任等級。透過使用 EV 的 VeriSign 安全網站專業版 SSL 憑證，您可以確保網站客戶和商業合作夥伴都能體驗最安全的保護 — 無論他們使用哪一種作業系統或瀏覽器版本。有了使用 EV 的 VeriSign 安全網站專業版，您的公司就可以達到促進電子商務成長所需的信任等級。

瀏覽器和安全服務供應商控制了顯示機制，以嚇阻企圖強奪您的品牌與客戶的網路釣客和仿冒者。詐騙集團愈來愈善於仿冒網站的每一項元素，但是如果沒有合法公司的 EV SSL 憑證，他們就無法在網址列顯示公司名稱，因為網址列所顯示的資訊已經超出他們的控制範圍，而且嚴格的驗證流程也讓他們無法取得合法公司的 EV SSL 憑證。

為什麼 EV 會讓消費者如此安心？

- 線上客戶可以查看網址列中憑證擁有者名稱的視覺顯示，確認網站確實是指定來源所架設，而不是冒牌網站。
- 如前面所述，在核發 EV 憑證給組織之前，CA 將會針對組織的合法性與正統性進行其他層面的驗證工作，使詐騙組織無法偽裝成合法的網際網路公司。
- CA 本身必須符合更嚴格的標準，才能取得核發 EV SSL 憑證的資格。他們必須通過第三方 WebTrust 定期審核，以確認他們符合 CA 與瀏覽器供應商共同組成之 CA/Browser Forum 的標準中所規定的要求事項。這種作法完全排除了因為背景調查不夠嚴謹讓冒牌網站通過 EV 驗證的機會。只要有 EV，客戶就不需要質疑組織是否已經過適當的調查。
- 將顏色變成綠色似乎可對客戶產生安撫的心理作用。即使客戶不熟悉為什麼 EV 能夠提供更妥善保護的「真正」原因，在看到綠色網址列時，他們的消費意願也會提高。

證明 EV 效果卓著的證據不勝枚舉。Tec-Ed 在 2007 年 1 月調查過 384 位線上購物者的使用狀況和態度，發現：

- 100% 的參與者會注意網站是否顯示綠色的 EV 網址列
- 93% 的參與者比較喜歡在顯示綠色網址列的網站購物
- 97% 的人願意在顯示綠色 EV 網址列的網站上分享信用卡資訊，相對地，只有 63% 的人願意在非 EV 網站上這樣做
- 77% 的參與者表示他們不太敢在本來顯示綠色 EV 網址列但現在卻沒有的網站上購物

在同一項研究中 Tec-Ed 發現，有 88% 的參與者信任網站上的 VeriSign 這個名稱，而相對地，只有 22% 信任第二大最受信任的 SSL 供應商。

類似的研究消除了對於 EV 價值和重要性以及有關消費者對於 VeriSign 這個名稱的認可、信任和喜好的所有懷疑。但是這可以轉變成更高的銷售量嗎？這個問題的答案也是肯定的，而且同樣有大量的證據足以佐證。許多 VeriSign EV SSL 憑證擁有者都會計算綠色網址列在銷售轉換率上所帶來的改變，而資料顯示：截至 2008 年 8 月為止，已有 14 位客戶的業績明顯提升，同時還有更多的報告不斷出爐。舉例來說，Overstock.com 發現在看到綠色網址列的購物者中，放棄購物車的人數下降了 8.6%。其他客戶業績提升的數字甚至更為驚人，包括有一位客戶對於他們的註冊率提高了 87% 感到十分驚喜。如需完整的詳細資料，請參閱 www.verisign.com/ssl/ssl-information-center/ssl-case-studies/index.html。

消費者將 VERISIGN 譽為網站安全性第一品牌。

所有的 VeriSign SSL 憑證都附有 VeriSign Secured 全球安全網站認證標章，可以讓您的公司顯示網際網路首屈一指的信任標誌。根據 TNS 在 2006 年 8 月所做的一項研究顯示，這個認證標章受到 79% 的美國線上購物者認可。值得注意的是，有 86% 的購物者表示顯示信任標記對網站來說非常重要。VeriSign Secured 全球安全網站認證標章也可以讓訪客即時查看您的 SSL 憑證的資訊和狀態 — 提高客戶對電子企業的信心。

+ VeriSign SSL 憑證，最堅實的安全與信任

VeriSign 是頂尖的 SSL 憑證全球供應商。VeriSign 無疑也是最重要的 EV SSL 憑證供應商，擁有的市場佔有率超過 75%，其中包括電子商務和銀行業界的龍頭⁷。全球最大的 40 家銀行和超過 95% 的《財星》前 500 大企業都選擇 VeriSign, Inc. 的 SSL 憑證⁸，而且遍及 145 個國家的 90,000 多個網域也都顯示網際網路上最受公認的信任標記 VeriSign® Secured 全球安全網站認證標章。網路使用者習慣看到電子商務網站顯示 VeriSign Secured 全球安全網站認證標章 — 當做顯眼的特徵，藉以向線上使用者保證他們的 Web 企業值得信任，而且網站能夠使用 SSL 加密來保護使用者的機密資訊。

為了因應各種不同需求，VeriSign 提供四種主要的 SSL 方案。

VeriSign 安全網站

這個最基本的 VeriSign 方案包括：

- 組織驗證
- 最低 40 位元至最高 256 位元加密
- 顯示 VeriSign Secured 全球安全網站認證標章的權利
- \$100,000 保固
- 安裝檢查工具

VeriSign 安全網站專業版

VeriSign® 安全網站專業版使每位網站訪客都能採用最強的加密。這個方案包含 VeriSign 安全網站加上 SGC 加密的所有技術，可為 99.9% 的網際網路使用者提供最少 128 位元的加密。包含 \$250,000 的保固。

使用 EV 的 VeriSign 安全網站

這個方案包含 VeriSign 安全網站加上延伸驗證的所有技術。延伸驗證 SSL 提供了一種簡單又可靠的方法，供網站訪客用來建立線上信賴關係。只有使用延伸驗證 (EV) 的 SSL 憑證才會讓高安全性 Web 瀏覽器顯示綠色網址列，以及擁有 SSL 憑證之組織的名稱與核發憑證之憑證管理單位的名稱。

使用 EV 的 VeriSign 安全網站專業版

使用 EV 的 VeriSign 安全網站專業版是最佳的 SSL 方案，可用來防止通訊對象以外的任何人讀取或修改進出網站的機密傳輸，而且能夠讓客戶產生信心。這個方案包含其他方案中的所有技術，包括 SGC 加密和 EV SSL 兩種憑證，以及 \$250,000 的保固。

VeriSign 建議的最佳加密與信任方案是使用 EV 的安全網站專業版 SSL 憑證。這個方案可讓高安全性的瀏覽器顯示 EV 綠色網址列，並讓所有的網站訪客都能以最高的加密等級進行連線。

⁷ Netcraft，2008 年 8 月

⁸ 包括 VeriSign 的子公司、聯盟機構與經銷商。

VeriSign 可以透過保護您的商務網站，幫助您的公司建立或提高客戶對您公司的信任。VeriSign SSL 憑證可以保護 Web 伺服器對用戶端、伺服器對伺服器，甚或其他網路裝置（例如伺服器負載平衡器或 SSL 加速器）之間的資訊交換。VeriSign 方案可以保護同時面對網際網路和私有企業內部網路的伺服器，藉以提供完整的跨網路安全機制。

+ 結論

隨著網際網路詐騙事件暴增，現今個人資料傳輸安全的重要性已非同日可語，而且未來的情況只會愈來愈嚴重。身分盜用的盛行 — 與後果 — 不僅眾所周知而且也有正式記錄。潛在的線上客戶變得愈來愈聰明、愈來愈多疑，其實也是愈來愈害怕。他們希望您能夠保護他們，而且目前有 84% 的人認為您並未採取足夠的保護措施⁹。

信任可以改變這一切。您在保護客戶及贏得客戶信任的技術上所做的投資只不過業務營運成本的一小部分，但是透過額外銷售所獲得的報酬率卻可能非常驚人 — VeriSign 有個客戶的報酬率即高達 48,000%（您可以在 VeriSign 的網站上參閱這位客戶和其他客戶的案例研究）。

當報酬如此龐大而成本又如此微小時，為什麼不做出正確的選擇呢？請選擇最知名也最受信任的名稱，因為知名度和信任感對 SSL 供應商來說非常重要。完善的安全防護措施讓 VeriSign 贏得知名度和信任，而且客戶也明白這一點。不要再裹足不前了 — 請直接選擇使用 EV 的 VeriSign 安全網站專業版 SSL 憑證，這樣您就可以告訴「所有」客戶他們的敏感資訊的傳輸過程沒有任何漏洞，而且傳輸目的地確實是他們希望傳送的對象。

+ 進一步瞭解

VeriSign 提供 www.verisign.com.hk 上說明的一系列額外電子商務網站服務，以符合每家線上企業的需求。如果想要和 VeriSign 安全專家討論貴公司的網站安全需求，請撥打免費電話 +800 8006 4000。您也可以透過電子郵件地址 sales@verisign.com.hk 與 VeriSign 聯絡。

+ 免費試用 VeriSign SSL 憑證

您可以使用為期兩週的免費試用版來保護您的網站。若要申請免費試用的 VeriSign 安全網站 SSL 憑證，請立即造訪 www.verisign.com.hk/trial。大約 15 分鐘後，您就可以完成完整的線上登錄程序，隨即開始使用您的 VeriSign SSL 憑證試用版。

+ 關於 VeriSign

VeriSign 是數位世界中，值得信賴的網際網路基礎架構服務供應商。各公司行號與消費者每天都安心地依賴我們的網際網路基礎架構，進行數十億次的通訊與商務活動。

欲知更多資訊，請造訪 www.Verisign.com.hk。

⁹ Forrester Research，2005 年 12 月