Transport Layer Security (TLS，傳輸層安全性)

關於 TLS

HSBC
The world's local bank

內容

滙豐安全電子郵件..... 2

關於 Transport Layer Security (傳輸層安全性) 2

設定與滙豐之間的 Forced TLS (強制 TLS) 連線 4

詞彙表 5

支援 5

滙豐安全電子郵件

在滙豐，我們致力於以最嚴格的資訊安全性標準來維護我們保有的資訊，並確保與您通訊時，依然妥善保護該資訊。因此我們在政策上規定，當電子郵件含有可能引發風險的資訊，都必須加密保護這些電子郵件，以免在遭他人攔截時，這些資訊使您或滙豐面臨風險。

一旦可行，滙豐就會利用稱爲 Transport Layer Security (TLS，傳輸層安全性) 的安全性通訊協定，從滙豐電子郵件帳戶寄送包含私密和敏感性資訊的滙豐電子郵件。

這種安全電子郵件解決方案會與我們的網路銀行服務分開運作。

關於 Transport Layer Security (TLS，傳輸層安全性)

Transport Layer Security (TLS，傳輸層安全性) 會利用標準加密技術來保護在網際網路上傳輸的電子郵件。以此種方式保護電子郵件，能減少攔截、竊聽和郵件僞造之風險。

TLS 如今已受多數的郵件伺服器應用程式所支援，而且有愈來愈多的組織實行這種方式，滙豐也是其中之一。

除了 TLS，如果您向我們註冊您的電子郵件網域細節，我們可以與您進行 Forced TLS 連線。如果我們與客戶的郵件伺服器達成安全連線，Forced TLS 能確保電子郵件只由我們寄送。

下列資訊詳述了 TLS 如何運作、誰適合使用 TLS，以及如何與我們建立 Forced TLS 連線。

什麼是 Transport Layer Security (TLS，傳輸層安全性)？

Transport Layer Security (TLS，傳輸層安全性) 是一種電子郵件安全工具，以 Secure Sockets Layer (SSL) 3.0 通訊協定爲基礎。它利用標準加密技術來保護在網際網路上傳輸的電子郵件。

TLS 如何運作？

要使 TLS 運作，必須在電子郵件寄件者和收件者的郵件伺服器上啓用 TLS。在伺服器之間交換的任何資訊都會進行加密，包括主旨列、文字和任何的附件。

在寄送加密訊息時，郵件交換的運作方式如下：

© HSBC Holdings plc 2011。保留所有權利

- 當寄件者連線至收件者時，系統會自動檢查客戶的郵件伺服器是否已啓用 TLS。
- 如果兩端都啓用了 TLS，會利用「交握」程序建立安全的 TLS 連線。
- 在交握期間，會交換 TLS 憑證。如果寄件者的伺服器信任來自客戶郵件伺服器的憑證，便會啓動 TLS 工作階段，並透過安全的網際網路連線來寄送電子郵件。

誰使用 TLS？

TLS 在短期內很快就會變成業界標準，而且多數的郵件伺服器應用程式現在都已提供支援。現在已有愈來愈多的組織實行這種方式，滙豐即是其中之一。

企業組織爲何使用 TLS？

TLS 已被證實是一個穩定且可靠的服務，一旦電子郵件寄件者和收件者的郵件伺服器上皆具有此服務，雙方便不需介入操作。這代表寄件者和收件者都能像現在一樣寄送和接收郵件。

基於這些原因，TLS 正快速成爲業界標準，許多尚未採用的金融機構也正打算執行 TLS。

什麼是 Forced TLS (強制 TLS)？

Forced TLS (強制TLS) 是一個可配置的 TLS 原則設定，它除了會遵循 TLS 程序外，還會將目的地電子郵件網域驗證爲信任的來源。如此能確保電子郵件只會以安全的方式傳送，而且其來源也是可信任的。

使用 TLS 還有哪些優點？

更強大的保護 – 能設定讓電子郵件伺服器強制執行 TLS (Forced TLS)。如此能確保將所有的電子郵件安全地寄送給信任的一方。滙豐的政策是，在任何可行的情況下與顧客、客戶和第三方建立 Forced TLS 連線。

可用性 – TLS 可用於多數的郵件伺服器上，而且是一種全球公認的電子郵件安全解決方案。

讓電子郵件接受防毒掃瞄 – 透過 TLS 傳送的訊息依然能像一般電子郵件一樣接受防毒掃瞄或惡意內容掃瞄。

減少成本 – 只要 TLS 已成爲組織的郵件伺服器功能，組織僅需購買年度 TLS 憑證即可，不像許多 點對點系統需要企業授權或個別使用者授權。

迅速部署 – TLS 可直接設定於郵件伺服器上，因此設定程序很簡單，不需進行個別工作站的設定。實施和測試工作僅需幾天的時間，不需花費數月。一旦設定 TLS，則能以往常的方式交換電子郵件。

建立與滙豐強制TLS (Forced TLS)的連線

由於 TLS 是設定於組織的郵件伺服器上，您應該與您的技術部門聯繫，瞭解是否已啓用 TLS。如果沒有，可以的話請您的技術部門啓用 TLS。

© HSBC Holdings plc 2011。保留所有權利

一旦設定好 TLS，您可以列出電子郵件網域以及您 IT 代表的連絡細節與您的滙豐客戶經理聯繫。您的滙豐客戶經理將轉寄這些細節給我們的 IT 部門，IT 部門會與您的 IT 代表協助進行 Forced TLS 連線測試。

我們也會積極與先前已和我們使用 TLS 方案的顧客、客戶及第三方合作，確保我們已擁有了透過 Forced TLS 寄送電子郵件所需的所有資訊。您可以選擇在您的組織使用相同的 Forced TLS 原則。如此一來，雙方隨時都將能安全地交換電子郵件。

© HSBC Holdings plc 2011。保留所有權利

詞彙表

電子郵件網域
電子郵件網域是電子郵件地址 @ 符號後面的部分。您的公司或許會有一個以上的電子郵件網域 (例如：hsbc.com、hsbc.com.hk)

電子郵件伺服器
電子郵件伺服器會先以某種方式處理傳入的電子郵件 (例如：過濾垃圾郵件)，之後才將其傳送至收件者的電子郵件收件匣。

加密
加密是一種轉換資料的程序，除了經授權能收到此資料的人以外，其他人都無法閱讀。

安全電子郵件
安全電子郵件是一種經過加密的電子郵件，使其能在網路上以安全方式寄送。

伺服器
伺服器是管理網路資源的電腦系統或裝置。伺服器通常作爲檔案的儲存裝置。

SSL – Secure Socket Layer (SSL，傳輸層安全性)
SSL 替網際網路通訊提供了加強的安全性。SSL 使用了**加密** (請見上方) 來確保敏感性資訊的機密性，像是信用卡號碼、帳戶餘額還有其他財務及個人資料，並在網路瀏覽器和網路**伺服器** (請見上方) 之間傳送這些資訊。

支援

請洽詢您的滙豐客戶經理或滙豐代表，他們可將您的問題轉給滙豐的相關團隊進行處理。

免責聲明

Transport Layer Security (TLS，傳輸層安全性) 是一種安全性通訊協定，以 Secure Sockets Layer (SSL) 3.0 通訊協定爲基礎。透過網際網路寄送的訊息，無法保證是完全安全的，因爲訊息可能會被攔截、遺失或變更。HSBC Holdings plc 和/或滙豐成員 (以下簡稱本公司) 不對客戶 TLS 的使用做出任何供應、維護、支援或授權之行爲，或以其他方式從中收取費用，因此也不做出任何代言或保證，包括保證未侵權、效能表現、使用時不受中斷、延遲、故障、錯誤、遺漏，或遺失傳輸資訊。當使用 TLS 在網際網路上寄送和接收訊息時，倘若發生問題或損害，本公司對這些問題或損害概不負責，也不承擔法律責任。

© HSBC Holdings plc 2011。保留所有權利

發佈方：HSBC Holdings plc
我們是滙豐集團的主要成員之一，滙豐是
是全球最大的銀行及金融服務機構之一，
我們在 87 個國家與地區設有大約 8,000 個辦事處。

出版者：集團資訊安全風險團隊，
HSBC Holdings plc
(8 Canada Square, London, United Kingdom E14 5HQ)

© HSBC Holdings plc 2011
保留所有權利