OPENTEXT™

移轉至 SHA-2 憑證

常見問題

如何使用本文件？

本常見問題解答了客戶針對從 SHA-1 移轉至 SHA-2 憑證方案最常提出的一些疑問。本文件將被託管於 http://www.opentext.com/campaigns/sha2。

什麼是 SHA-2？

SHA-2 是一種密碼雜湊演算法，在 2001 年由美國國家安全局首次發佈。SHA 代表的是安全雜湊演算法。SHA 雜湊函數被使用於如 TLS 與 SSL 的安全性應用程式及通訊協定，並在針對加密及數位簽署時與公開金鑰演算法結合使用。

為何 OpenText 要從 SHA-1 轉換至 SHA-2 憑證？

隨著密碼攻擊的進展，網路安全專家已警告，使用 SHA-1 憑證可能會使攻擊者得以詐騙內容、執行網路釣魚攻擊或「中間人攻擊」。雖然此潛在漏洞不存在於 OpenText™ Trading Grid™、OpenText Information Exchange, OpenText EasyLink GMS 或 OpenText EasyLink ICC.Net，但是爲了持續提供給客戶最高的資料完整性與安全性，我們仍然將移動至 SHA-2 憑證。

SHA-2 中使用的加密雜湊明顯較強，且沒有如同 SHA-1 的漏洞。

如需瞭解您的內部系統是否支援 SHA-2，請造訪 https://www.digicert.com/sha-2-compatibility.htm

OpenText 採取哪些措施以移動至 SHA-2？

當目前的憑證過期後，OpenText 將開始更新所有的憑證為 SHA-2。我們計劃截至 **2017 年 1 月 1 日**將 SHA-1 完整地移轉至 SHA-2 憑證，此日期則是 Microsoft® 已宣告將停止支援 SHA-1 憑證的日期。SHA-2 憑證將透過我們目前的憑證授權單位 Comodo 發行。

注意：*我們有權利保留升級實際執行前的環境憑證（過期前），以給予客戶與其貿易合作夥伴測試的時間。*

對我有什麼影響？

如果您或您的貿易合作夥伴使用 FTPS、AS2、RosettaNet、OFTP、MQ、AS3 或其他通訊協定以與 Trading Grid™、Information Exchange, EasyLink GMS 或 EasyLink ICC.Net 建立一個數位簽署或已加密的訊息交換連線，OpenText 建議您開始準備將 SHA-1 憑證替換至 SHA-2 憑證以增強安全性保護。

我必須採取哪些措施？

為準備此變更並確保順利執行憑證更新程序：

1. 與您的服務或軟體供應商確認，確保您的通訊軟體支援由 Comodo 發行的 SHA-2 憑證。

a. 如果支援，當您目前的 OpenText 公開金鑰憑證過期後，您將可協調移轉至更安全的 SHA-2 憑證。
b. 如果不支援，而您目前的通訊軟體供應商無法協助您，則請聯絡您的 OpenText 客戶經理以討論適用於您的選項。

2. 聯絡您的貿易合作夥伴並使他們與其通訊軟體供應商執行相同的驗證，以確保他們的通訊軟體支援由 Comodo （我們目前的憑證授權廠商）發行的 SHA-2 憑證。

憑證更新程序將變更嗎？

不會對憑證更新程序進行變更。然而，OpenText 可能會在憑證過期前將其更新為 SHA-2，以在 2017 年 1 月 1 日的截止日期前確保相容性。

如果目前的公開金鑰憑證於 2016 年 12 月 31 日後過期該怎麼辦？

OpenText 將致力聯絡仍在使用目前 OpenText 公開金鑰 SHA-1 憑證的客戶，幫助他們在 2017 年 1 月 1 日的截止日期前移轉至 SHA-2 憑證。

受此變更影響的服務有哪些？

此變更影響所有 SSL 瀏覽憑證以及特定通訊協定。如果您透過現代網頁瀏覽器連接至 OpenText，則將不會受憑證升級影響。

注意：*這目前不影響 SSH、PGP 或 GPG 加密金鑰。*

受此變更影響的通訊協定右哪些？

被移轉至 SHA-2 憑證所影響的通訊協定如下：

- AS2
- AS3
- HTTP over SSL
- SSL-FTP (FTP over SSL)
- RosettaNet
- MQ
- Sterling/IBM – Connect:Direct Secure Plus

OpenText 目前支援哪些 SHA-2 雜湊函數？

OpenText 目前支援透過以下 SHA-2 版本所簽署的憑證：

- SHA256
- SHA384
- SHA512

將來，OpenText 則計劃支援更多的 SHA-2 憑證類型。當他們變得可支援後，我們將會通知與其相關的更多細節。

我的通訊軟體無法支援 SHA-2 憑證。我該怎麼辦？

雖然 OpenText 建議，幫助維持資料完整性與安全性最有效的方式就是移轉至 SHA-2 憑證，但是我們知道，並非所有的客戶能夠支援 SHA-2 憑證。

如果您的軟體不支援 SHA-2 或自我簽署憑證，憑證交換團隊將協助您，提供您一個為期一年的替代方案。2015 年 12 月 31 日後，OpenText 將不會再提供替代的憑證發行選項。2016 年起，憑證交換團隊將停用所有的 SHA-1 憑證發行選項，並需要客戶移動至 SHA-2 或自我簽署憑證。如果到時您仍讓無法支援 SHA-2 憑證，憑證交換團隊將協助您實施一個自我簽署的 SHA-1 憑證。

憑證交換團隊

電子郵件：CertificateExchange@opentext.com
電話：1-800-334-2255 x2378 (CERT)

什麼是 Comodo？

Comodo 是 OpenText 的主要憑證授權單位。憑證授權單位是發行並管理數位憑證的組織。如需更多資訊，請造訪 Comodo 網站：www.comodo.com。

OpenText 為何切換至 Comodo？

OpenText 選擇 Comodo 是因為其提供完整的數位憑證系列（提供最強的加密功能），並具有迎合企業需求的技術能力與彈性。作為一個網路安全憑證授權單位 (CA)，Comodo 符合最高標準的機密性、系統可靠性，以及透過合格獨立稽核的特定業務實踐。

切換至 Comodo 會對我的服務造成影響嗎？

切換至 Comodo 發行的憑證應對較新的檔案交換產品造成極小的影響。Comodo 是個相對新的的憑證授權單位，因此使用舊版檔案交換產品（少於 10 年）的客戶可能無法將根與中繼憑證載入憑證存放區。如需更多資訊，請造訪 Comodo 網站：www.comodo.com。

注意：*使用舊版檔案交換產品或自我開發軟體的客戶應載入所有鏈結憑證 (.p7b)。如果您使用 .cer 版本，請確保全三種 Comodo 憑證已載入您的憑證存放區。*

我應該向誰索取進一步資料？

如需更多資訊，OpenText Trading Grid/Information Exchange 客戶可聯絡 Cloud Support Services。

OpenText EasyLink GMS 與 ICC.Net 客戶可聯絡 OpenText EasyLink Customer Support.

僅為 Sterling Connect:Direct 使用者

如何知道我的 Sterling Connect:Direct 軟體版本是否與 SHA-2 相容？

如需更多 SHA-2 支援（針對 Sterling Connect:Direct）資訊，請在 IBM 網站上參考 SHA-2 支援指南。您可透過造訪以下連結存取指南：

ftp://ftp.software.ibm.com/software/commerce/doc/mft/cdcommon/secplus_SHA2SupportForCD_Book.pdf

請參考***表格 2***。參考 ***SHA-2 相容軟體*** 以查看您的 Connect:Direct 版本是否支援 SHA-2。如果您的版本與 SHA-2 不相容，我們則為您提供幾個選項。這些選項包括：

1. 將您的 Connect:Direct 軟體升級至一個支援 SHA-2 的版本。
2. 聯絡您的 OpenText 代表以安裝 / 設定另一個通訊協定，從而進行資料傳輸。

注意：如果您透過 OpenText 僅傳送**輸入**檔案，則可能不會有任何問題。然而，除非您的系統能夠支援 SHA-2 憑證，OpenText 將無法傳送您任何資料檔案。

使用 Connect:Direct 連接至 OpenText 的標準必要條件有哪些？

標準必要條件包括：

- OpenText 僅安裝 / 加入客戶的根憑證和 / 或中繼憑證至我們信任的存放區。
- 傳送至 OpenText 的憑證不應是自我簽署憑證。OpenText 將不接受自我簽署憑證。
- 應關閉用戶端驗證
- OpenText 偏好 Base64 編碼格式的憑證。
- 應加入所有加密套件至 Secure+ 設定
- OpenText 已設定用於 TLSv1

為與 OpenText 進行連線，我需要在 Connect:Direct 系統內安裝的憑證有哪些？

客戶將需要安裝以下的新憑證為獨立檔案：

- 公開憑證（應包含鏈結中的憑證）
- 中繼憑證（應包含僅有根 CA 的鏈結）
- 根 CA 憑證

我應對新憑證採取哪些措施？

客戶應安裝 / 加入適用憑證至他們 OpenText 的 Connect:Direct 節點 Secure+ 設定 或與他們的內部技術聯絡人和 / 或 IBM 支援進行諮詢。

是否移除您之前的憑證？

移除之前憑證的需求相依於您特定的 Connect:Direct Secure+ 設定。請與您的內部技術聯絡人和 / 或 IBM 支援進行諮詢。

還需其他 Secure+ 設定支援 SHA-2 憑證嗎？

不需要。然而，客戶可選擇以下變更選項。

- 將所有加密套件加至 Secure+ 設定
- 移除弱式或已中斷加密套件

我需要使用 SHA-2 憑證進行測試嗎？

OpenText 建議客戶針對新憑證進行測試，以確保他們如期進行作業。如果遇到問題，客戶應使用 Cloud Support Services 開啟產品服務要求。

如果我的憑證過期該怎麼辦？

一個過期的憑證通常意味著公開憑證，而非中繼或根 CA，已過期。許多情況下，您無需對實際憑證進行任何措施，因為中繼和 / 或根 CA 並無變更。如果中繼和 / 或根 CA 是新的，則請將他們加入信任的存放區。

About OpenText

OpenText enables the digital world by simplifying, transforming, and accelerating enterprise information needs, on premises or in the cloud. For more information about OpenText Cloud Services (NASDAQ: OTEX, TSX: OTC) visit www.gxs.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn | Facebook

www.gxs.com/support | www.easylink.com/support

NORTH AMERICA +800 334 2255 • UNITED STATES +1 301 251 65100

OTHER LOCATIONS http://techsupport.gxs.com/regional-directories