



客戶報告

OpenText™ 從 SHA-1 至 SHA-2 的憑證移轉

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™/Information Exchange 本身，但是我們仍然發行此諮詢以持續提供客戶最高的資料完整性與安全性。

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 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。

為幫助客戶移動至 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。

需執行的動作

為準備此變更並確保順利執行憑證更新程序：

1. 與您的軟體供應商確認，確保您的通訊軟體支援由 Comodo 發行的 SHA-2 憑證。
 - 如果支援，當您目前的 OpenText 公開金鑰憑證過期後，您將可移轉至更安全的 SHA-2 憑證。
 - 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。

在 OpenText，我們視您的資訊安全性與私密性為我們的第一要務。因此，我們將繼續評估我們的軟體產品，並採取必要的動作以防止所有資料安全性威脅。

更多資訊

如需更多資訊，請參考 [常見問題](#) 或聯絡 [雲端支援服務](#)。

Copyright ©2015 Open Text Corporation. All Rights Reserved. OpenText is a trademark or registered trademark of Open Text SA and/or Open Text ULC. The list of trademarks is not exhaustive of other trademarks, registered trademarks, product names, company names, brands and service names mentioned herein are property of Open Text SA or other respective owners. All rights reserved. For more information, visit: <http://www.opentext.com/2/global/site-copyright>.