Migration zu SHA-2-Zertifikaten

Häufig gestellte Fragen (FAQ)

Wie verwende ich dieses Dokument?

Dieses Dokument (FAQ) enthält Antworten zu einigen der Fragen, die von unseren Kunden am häufigsten zur Umstellung der SHA-1- auf SHA-2-Zertifikate gestellt werden. Dieses Dokument wird unter http://www.opentext.com/campaigns/sha2 bereitgestellt.

Was ist SHA-2?

SHA-2 ist ein kryptografischer Hash-Algorithmus, der im Jahr 2001 erstmals von der US-amerikanischen National Security Agency veröffentlicht wurde. SHA steht für Secure Hash Algorithm, englisch für „Sicherer Hash-Algorithmus“. SHA-Hash-Funktionen werden in Sicherheitsanwendungen und -protokollen wie beispielsweise TLS und SSL verwendet sowie im Zusammenhang mit Public-Key-Algorithmen für Verschlüsselung und digitale Signaturen.

Weshalb wechselt OpenText von SHA-1- zu SHA-2-Zertifikaten?

Hinsichtlich der jüngsten Entwicklungen im Bereich der kryptografischen Angriffe haben Experten für Netzwerksicherheit eine Warnung für SHA-1-Zertifikate herausgegeben. Diese können es Angreifern ermöglichen, Inhalte zu fälschen sowie Phishing- oder „Man-in-the-Middle“-Angriffe durchzuführen. Obwohl diese potenzielle Sicherheitslücke nicht im direkten Zusammenhang mit OpenText™ Trading Grid™, OpenText Information Exchange, OpenText EasyLink GMS oder OpenText EasyLink ICC.Net steht, wechseln wir im Rahmen unserer kontinuierlichen Bemühungen zur Sicherstellung der höchsten Standards bei Datenintegrität und -sicherheit für unsere Kunden zu SHA-2-Zertifikaten.

Der in SHA-2 verwendete Sicherheits-Hash ist wesentlich stärker und weist keine der Sicherheitslücken von SHA-1 auf.

Informationen dazu, ob Ihre internen Systeme SHA-2 unterstützen, finden Sie unter https://www.digicert.com/sha-2-compatibility.htm

Was unternimmt OpenText, um zu SHA-2 zu wechseln?

Bei Ablauf der derzeit verwendeten Zertifikate ersetzt OpenText diese mit SHA-2-Zertifikaten. Geplant ist, die Umstellung der SHA-1- auf SHA-2-Zertifikate bis **1. Januar 2017** abzuschließen. Zu diesem Termin hat Microsoft® angekündigt, den Support für SHA-1-Zertifikate einzustellen. SHA-2-Zertifikate werden von unserer derzeitigen Zertifizierungsstelle Comodo ausgestellt.

Hinweis: *Wir behalten uns das Recht vor, Zertifikate aus Vorproduktionsumgebungen vor deren Ablauf zu aktualisieren, damit Kunden die notwendige Zeit erhalten, diese mit ihren Geschäftspartnern zu testen.*

Inwiefern bin ich davon betroffen?

Falls Sie oder Ihr Geschäftspartner FTPS, AS2, RosettaNet, OFTP, MQ, AS3 oder ein anderes Protokoll zum Aufbau einer digital signierten oder verschlüsselten Nachrichtenaustauschverbindung mit Trading Grid™, Information Exchange, EasyLink GMS oder EasyLink ICC.Net verwenden, empfiehlt OpenText, sich auf den Ersatz Ihrer SHA-1-Zertifikate mit SHA-2-Zertifikaten vorzubereiten, um die Sicherheit zu verbessern.

Was muss ich tun?

So bereiten Sie sich auf den Wechsel vor und unterstützen eine reibungslose Zertifikatserneuerung:

1. Fragen Sie bei Ihrem Dienst- oder Softwareanbieter nach, ob Ihre Kommunikationssoftware SHA-2-Zertifikate von Comodo unterstützt.
    a. Falls ja, sind Sie bereit, Ihre Umstellung auf das sicherere SHA-2-Zertifikat bei Ablauf Ihres derzeit verwendeten Public-Key-Zertifikats von OpenText zu koordinieren.
    b. Falls nein, und wenn Ihnen Ihr aktueller Kommunikationssoftwareanbieter nicht behilflich sein kann, wenden Sie sich bitte an Ihren Kundenbetreuer von OpenText, um Ihre verfügbaren Optionen zu besprechen.
2. Bitten Sie Ihre Geschäftspartner, ebenfalls bei ihren Kommunikationssoftwareanbietern sicherzustellen, dass ihre Kommunikationssoftware SHA-2-Zertifikate von Comodo, unserer derzeitig verwendeten Zertifizierungsstelle, unterstützt.

Ändert sich der Vorgang zur Zertifikatserneuerung?

Es gibt keine Änderungen beim Vorgang zur Zertifikatserneuerung. Es ist jedoch möglich, dass OpenText Zertifikate vor der Frist vom 1. Januar 2017 durch SHA-2-Zertifikate ersetzt, selbst wenn diese ihren Ablauftermin noch nicht erreicht haben.

Was geschieht, wenn mein aktuelles Public-Key-Zertifikat von OpenText nach dem 31. Dezember 2016 abläuft?

OpenText kontaktiert Kunden mit aktuellen Public-Key-SHA-1-Zertifikaten von OpenText proaktiv, um ihnen dabei zu helfen, die Umstellung auf SHA-2-Zertifikate vor der Frist vom 1. Januar 2017 durchzuführen.

Welche Dienstleistungen sind von dieser Umstellung betroffen?

Diese Umstellung betrifft alle SSL-Browserzertifikate und bestimmte Kommunikationsprotokolle. Wenn Sie sich über einen modernen Webbrowser mit OpenText verbinden, sind Sie vom Zertifikatsupgrade nicht betroffen.

Hinweis: *DSSH-, PGP- oder GPG-Verschlüsselungscodes sind derzeit davon ausgenommen.*

Welche Protokolle sind von dieser Umstellung betroffen?

Die folgenden Protokolle sind von der Umstellung auf SHA-2-Zertifikate betroffen:

- AS2
- AS3
- HTTPS
- SSL-FTP (FTPS)
- RosettaNet
- MQ

- Sterling/IBM – Connect:Direct Secure Plus

Welche SHA-2-Hashfunktionen werden derzeit von OpenText unterstützt?

OpenText unterstützt derzeit Zertifikate, die von den folgenden SHA-2-Versionen signiert sind:

- SHA256
- SHA384
- SHA512

Zukünftig plant OpenText auch die Unterstützung weiterer SHA-2-Zertifikatsarten. Weitere Details werden mit ihrem Erscheinen bekannt gegeben.

Meine Kommunikationssoftware bietet keine Unterstützung für SHA-2-Zertifikate. Was soll ich tun?

OpenText empfiehlt zwar die Umstellung auf SHA-2-Zertifikate als effektivstes Verfahren zur Beibehaltung von Datenintegrität und -sicherheit, ist sich jedoch der Tatsache bewusst, dass nicht alle Kunden SHA-2-Zertifikate unterstützen können.

Wenn Ihre Software keine Unterstützung für SHA-2- oder selbstsignierte Zertifikate bietet, arbeitet das Certificates Exchange Team gemeinsam mit Ihnen daran, Ihnen bis zu einem Jahr lang eine Alternative bereitzustellen. Nach dem 31. Dezember 2015 stellt OpenText keine alternativen Zertifikatoptionen mehr bereit. Ab 2016 deaktiviert das Certificates Exchange Team alle Ausstelloptionen für SHA-1-Zertifikate, sodass ein Wechsel zu einem SHA-2- oder selbstsignierten Zertifikat für alle Kunden verpflichtend ist. Wenn Sie zu diesem Zeitpunkt immer noch keine SHA-2-Zertifikate unterstützen können, arbeitet das Certificates Exchange Team gemeinsam mit Ihnen daran, ein selbstsigniertes SHA-1-Zertifikat zu implementieren.

Certificates Exchange Team

E-Mail: CertificateExchange@opentext.com
Telefon: 1-800-334-2255 x2378 (CERT)

Was ist Comodo?

Comodo ist die zentrale Zertifizierungsstelle von OpenText. Zertifizierungsstellen sind Organisationen, die digitale Zertifikate ausstellen und verwalten. Weitere Informationen finden Sie auf der Webseite von Comodo unter www.comodo.com

Weshalb wechselte OpenText zu Comodo?

OpenText wählte Comodo aus, weil das Unternehmen eine vollständige Palette digitaler Zertifikate mit der derzeit besten verfügbaren Verschlüsselung anbietet sowie die technischen Ressourcen und die Flexibilität besitzt, den Anforderungen der Geschäftswelt gerecht zu werden. Als WebTrust-Zertifizierungsstelle (CA) erfüllt Comodo die höchsten Standards für Vertraulichkeit, Systemsicherheit und entsprechende Geschäftspraktiken durch qualifizierte unabhängige Kontrollen.

Kann sich der Wechsel zu Comodo auf meine Dienstleistungen auswirken?

Der Wechsel zu einem Comodo-Zertifikat sollte keinen Einfluss auf neuere Dateiaustauschprodukte haben. Da es sich bei Comodo um eine relativ neue Zertifizierungsstelle handelt, können bei Kunden mit älteren Dateiaustauschprodukten (>10 Jahre) Probleme beim Laden der Root- und Zwischenzertifikate im Zertifikatsspeicher auftreten. Weitere Informationen finden Sie auf der Webseite von Comodo unter www.comodo.com.

***Hinweis**: Kunden mit älteren Dateiaustauschprodukten oder eigens entwickelter Software sollten alle verketteten Zertifikate laden (.p7b). Wenn Sie die CER-Versionen verwenden, müssen Sie sicherstellen, dass alle drei Comodo-Zertifikate in Ihrem Zertifikatsspeicher geladen sind.*

An wen kann ich mich wenden, um weitere Informationen zu erhalten?

Weitere Informationen erhalten OpenText Trading Grid- und Information Exchange-Kunden von Cloud Support Services.

OpenText EasyLink GMS- und ICC.Net-Kunden können sich an den OpenText EasyLink Customer Support wenden.

Nur für Benutzer von Sterling Connect:Direct

Wie erkenne ich, ob meine Sterling Connect:Direct-Softwareversion mit SHA-2 kompatibel ist?

Weitere Informationen zum SHA-2-Support für Sterling Connect:Direct erhalten Sie in der SHA-2 Support-Anleitung auf der Webseite von IBM. Sie können die Anleitung auch über folgenden Link öffnen:

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

Siehe ***Tabelle 2: SHA-2-kompatible Software***, um zu erfahren, ob Ihre Connect:Direct-Version Unterstützung für SHA-2 bietet. Wenn Ihre Version nicht mit SHA-2 kompatibel ist, stehen Ihnen mehrere Optionen zur Verfügung. Dazu gehören:

1. Upgrade Ihrer Connect:Direct-Software auf eine Version, die SHA-2 unterstützt
2. Installation/Konfiguration eines anderen Protokolls zur Datenübertragung durch Ihren OpenText-Kundenbetreuer

Hinweis: Wenn Sie nur **Inbound**-Dateien über OpenText versenden, treten in der Regel keine Probleme auf. Allerdings kann OpenText Ihnen nur dann Datendateien zusenden, wenn Ihr System SHA-2-Zertifikate unterstützt.

Was sind die Standardvoraussetzungen für die Verbindung mit OpenText mithilfe von Connect:Direct?

Zu den Standardvoraussetzungen gehören:

- OpenText installiert nur Root-CA- und/oder Zwischenzertifikate des Kunden in unserem Truststore
- An OpenText gesendete Zertifikate sollten nicht selbstsigniert sein. OpenText akzeptiert keine selbstsignierten Zertifikate
- Die Client-Authentifizierung sollte deaktiviert sein
- OpenText bevorzugt Zertifikate im Base64-Verschlüsselungsformat
- Alle Cipher-Suites sollten dem Secure+-Setup hinzugefügt werden
- OpenText ist für TLSv1 konfiguriert

Welche Zertifikate muss ich auf meinem Connect:Direct-System installieren, um eine Verbindung mit OpenText zu erzielen?

Kunden müssen die folgenden neuen Zertifikate als eigene Dateien installieren:

- Öffentliches Zertifikat (sollte die Zertifikate in der Kette beinhalten)
- Zwischenzertifikat (sollte die Kette mit nur dem Root-CA beinhalten)
- Root-CA-Zertifikat

Was soll ich mit den neuen Zertifikaten tun?

Kunden sollten die entsprechenden Zertifikate im Secure+-Setup für den Connect:Direct-Knoten von OpenText installieren/hinzufügen oder sich an ihren internen technischen Ansprechpartner bzw. den IBM Support wenden.

Muss ich alte Zertifikate entfernen?

Ob Sie alte Zertifikate entfernen müssen, hängt von Ihrem jeweiligen Connect:Direkt Secure+-Setup ab. Wenden Sie sich an Ihren internen technischen Ansprechpartner bzw. den IBM Support.

Werden weitere Secure+-Einstellungen zur Unterstützung von SHA-2-Zertifikaten benötigt?

Nein. Bei Bedarf können Kunden jedoch die folgenden Änderungen durchführen.

- Alle Cipher-Suites dem Secure+-Setup hinzufügen
- Ineffektive oder beschädigte Cipher-Suites entfernen

Muss ich das SHA-2-Zertifikat testen?

OpenText empfiehlt Kunden, ihre neuen Zertifikate zu testen, um deren ordnungsgemäße Funktion sicherzustellen. Falls Probleme auftreten, sollten Kunden eine Produktserviceanfrage bei Cloud Support Services öffnen.

Was geschieht, wenn mein Zertifikat abläuft?

Wenn ein Zertifikat abläuft, bedeutet dies in der Regel, dass zwar das Öffentliche Zertifikat abgelaufen ist, jedoch nicht das Zwischen- oder Root-CA. Meist müssen Sie nichts mit den einzelnen Zertifikaten tun, weil das Zwischen- und/oder Root-CA nicht verändert wurden. Wenn das Zwischen- und/oder Root-CA neu sind, fügen Sie sie dem Truststore hinzu.

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